

العدد رقم 11

NetworkSet

February 2011

NetworkSet Magazine

أول مجلة عربية مجانية تختص بأمور الشبكات
www.Networkset.net

مؤسس ورئيس تحرير المجلة : م.أيمن النعيمي

المحررون

المهندس أيمن النعيمي

www.NetworkSet.net

المهندس أنس الأحمد

EE4its@hotmail.com

المهندس إسلام محمد

Csi_Eslam@Yahoo.com

المهندس علاء مازن عدي

alaamazen@hotmail.com

المهندسة صفا الرمضاني

المهندس نادر المنسي

naderelmansi@gmail.com

المهندس شريف مجدي

sh8090@gmail.com

التصميم والإخراج الفني

صدى
Echo Technology

Integratoin Technical Solution

eng.Anas kh Al-Ahmad

الآراء المنشورة تعبر عن وجهة نظر الكاتب ولا تعبر عن وجهة نظر المجلة
جميع المحتويات تخضع لحقوق الملكية الفكرية
لا يجوز النقل دون إذن من المجلة أو الكاتب

المكتبيات

المحتويات	2
المبادرة	3
step secure Cisco 5	4
Mikrotik Router OS	6
DNS cache poisoning	10
network diagram	13
Network Troubleshooting using OSI Model	18
intrusion detection and prevention systems	22
خلق - علم - عمل	25
الإرسال والإستقبال من خلال الكابل	26
منهجية حل مشاكل الشبكة	28
نبذة عن الاسكي	30

المبادرة

هي كلمة بحثت عنها كثيرا ولم أتوصل إليها إلا مؤخرا مع انها أحد الصفات التي أحب أن أوصف بها دائما إلا أن فهمتها بعد أن وصلتني رسالة من المهندسة صفا الرمضاني التي أصبحت أحد المحررين معنا في المجلة وما أعجبني في رسالتها أنها لم تكن من النوع المألوف الذي اتلقاه دوما حول الاشتراك في المجلة فعادة ماتصلني رسائل تتطلب مني الاشتراك في المجلة ويتبعها رسالة عن المواضيع التي يمكن الكتابة عنها في المجلة ويتبعها اقتراحات والخ...وهو مايسبب حيرة لي أحيانا فأنا لا أعلم أمكانية كل واحد منهم ولا مستواه الحقيقي في عالم الشبكات إلا أن المهندسة صفا خالفت كل هذه الرسائل وقامت بأرسال المقال مباشرة وطلبت مني قراءة المقال وتحديد هل هو من النوع المناسب أم لا؟؟!! وأول ما كتبتة كان شكرا لكي على المبادرة الجميلة والمباشرة وهنا فقط تذكرت أن كلمة مبادرة هي الكلمة التي كنت أبحث عنها وهي ما أردت إيصاله لكم اليوم لأن المبادرة هي أكثر ما ينقصنا للأبداع والتميز وخصوصا أن الكثير من طاقتنا العربية خاملة وتحتاج إلى من يثيرها ولو نظرنا إلى المعنى الحقيقي لكلمة مبادرة في القاموس العربي لوجدنا أنها تشير إلى الأسراع في عمل ما بدون ملاحظة وهذا أن كان يدل على شيء فهو يدل على العمل الجاد والرغبة في تنفيذ شيء ما أما المماطلة فهي تدل على شيء واحد وهو الكسل والخمول ولأطرح عليكم مثال عملي أجده تقريبا كل أسبوع على المنتديات العربية ويفشل فشلا زريعا.

تفتح المنتدى وتجد موضوع عنوانه كالاتي " كل واحد يقوم بوضع معلومات عن كوابل الشبكات " أو " الموضوع الأوحده لكل المشاكل التي تمر بك في الحياة العملية " فكرة هذه المواضيع جميلة لكن لو فتحت ونظرت ماهو مكتوب بها لما فتحتها مرة أخرى فعلا سبيل المثال تجد أن الموضوع الاول يملك أكثر من عشرين رد وكلهم يؤيد الفكرة وهناك من يشكر صاحب الموضوع على الفكرة الجهنمية وهناك من يقول بانتظار باقي الأعضاء والكل يجلس ينتظر أصحاب الخبرات العالية والأشخاص الذين ولدوا وهم يحملون كابل للشبكة ويختفي الموضوع بعد أسبوع لتنتهي معه حكاية كوابل الشبكة . من وجهة نظري هذه الافكار يجب أن تموت لأن الشخص الذي بادر وكتب هذا الموضوع لم يعمل فيه فهدفه سلبي وهو معرفة أنواع الكوابل فقط من خلال موضوع وهمي يذكر فيه أنه لأفادة الآخرين والحقيقة غير ذلك والسبب لأنه لم يبادر بكتابة أي كلمة تفيد الموضوع ونفس الشيء يحدث مع باقي المواضيع فهي تحتاج من صاحبها أن يكون من اكثر الناس مساهمة فيه وليس متفرج يملك أفكار وهمية وخصوصا أن الأفكار والمواضيع كثيرة ولكن جميعها تنتظر مبادر حقيقي لكي يطرحه وليس مستهلك ذو عقلية متحجرة .

الخلاصة التي أريد أن أوصلها لك أخي القارئ كن مبادر ومبادر إيجابي وأعمل وأجتهد حتى تصل إلى مبتغاك ولا تكن مجرد نقطة على السطر توضع في آخر الكلام وحاول أن تشعر دائما بمثل ما أشعر عندما أطرح على نفسي السؤال الصغير أين نحن والغرب أين؟؟ هل ياترى أن بإمكانني أن أثبت للعالم أننا لسنا مستهلكين؟؟ هل أنا قادر على التغيير؟؟ كل هذه الأسئلة لا تقرأها مجرد قرأه بل أشعر بها وعندها سوف تأخذ الطاقة التي سوف تجعلك مبادر حقيقي وإيجابي.

أنطلق مشروعني الجديد لعمل أكبر موسوعة عربية في الشبكات وهي مبادرة جديدة مني لتغيير الواقع والمحتوى العربي وهي تحتاج إلى الكثير من المبادريين لأنجاحه لكن أن لم أجد من يبادر ثقوا أن هذه الموسوعة لن تتوقف يوما واحدا عن الاتساع أن شاء الله .

5 Step *secure Cisco*

الخطوة الثانية

تشفير كل كلمات السر

عندما نقوم بعرض الإعدادات الموجودة على الروتر من خلال الأمر Show Run سوف نلاحظ أن كل كلمات السر الموجودة غير مشفرة ماعدا ال Secret التي تحدثنا عنها من قبل أما باقي الكلمات فتكون كلها Clear Text وهذا يشمل كلمة السر الخاصة بالتلنت والكونسول والأكسيلاري وال Enable Password لذلك تعتبر خطوتنا الثانية هي تشفير هذه الكلمات من خلال كتابة الامر التالي في ال Configuration Mode :

```
Router(config)# service password-encryption
```

الخطوة الثالثة

تحديد كلمة سر خاصة بالكونسول.

يعتبر منفذ الكونسول سلاح ذو حدين فهو المنفذ الوحيد الذي يمكن من خلال أسترجاع كلمة السر للدخول إلى الروتر وفي نفس الوقت يكون غير محمي بأي كلمة سر عند أستخدامه لأول مرة لذلك خطوتك الثالثة سوف تكون حماية منفذ الكونسول من الأشخاص الغيوريين والذين يتربصون بك في مكان العمل وذلك من خلال الأوامر التالية :

```
Router(config)# line con 0
```

```
Router(config-line)# login
```

```
Router(config-line)# password your password
```



على نفس الأسلوب الذي أتبعته من قبل في طرحي لموضوع خمس خطوات يجب أن تعرفها حول سويتشات سيسكو أعود إليكم لكي أستعرض معكم أهم خمس خطوات يجب على مدير الشبكة أتخاذها لتأمين الشبكة التي تستخدم أجهزة سيسكو ومما لاشك فيه أن خطوات الحماية أكثر من هذا بكثير إلا أن هذه الخطوات تعتبر هي الأساس في عملية حماية الشبكة والأجهزة الموجودة عليها .

الخطوة الأولى

تشفير كلمة السر الخاصة بالدخول على الروتر

يصاب الكثير من المبتدئين في عالم سيسكو بالأرتباك بين امر ال Enable Password وأمر ال Enable secret Password والفكرة ببساطة تقول أن كلمة السر هذه هي للمكان نفسه وهي تستخدم للدخول إلى الروتر أو إلى السويتش ولكن الفرق بينهما أن الاولى لاتشفّر عند عرض الأمر Show Run بينما كلمة السر الخاصة بالأمر الثاني يتم تشفيرها ومن الصعب جدا كسرهما ولو في حال قمنا بكتابة كلا الأمران فأن الروتر سوف يأخذ كلمة السر الثانية الخاصة بي ال Secret Password لذلك أول خطوة سوف نقوم بها هي وضع كلمة سر من النوع المشفر من خلال الأمر التالي :

```
Router(config)# enable secret your password
```

أيمن التميمي

الخطوة الخامسة

تأمين المنافذ الموجودة على السويتش

في أحصائية قراتها منذ فترة تبين أن تسعين بالمئة من السويتشات الموجودة على الشبكة منافذها الغير مستخدمة تعمل ولم يتم إيقافها وهي أيضا أحد الأخطاء الشائعة جدا عند مهندسي أجهزة سيسكو لذلك خطوتك الخامسة سوف تكون أطفاء كل المنافذ الموجودة على السويتش من خلال الدخول على المنفذ وكتابة الامر Shutdown

إلى نكون قد أنهينا من حديثنا وأرجع وأقول أن الخطوات الخاصة بتأمين الشبكات أكثر من ذلك بكثير لكن تعتبر هذه الخطوات من الأشياء التي يجب أن تقوم بها أولا وبعدها تفكر في الخطوات الثانوية والتي من بينها أعداد ال Vlan وال Port Security والخ... أتمنى أن تكونوا قد استفدتم وأن أكون قد وفقت في إيصال المعلومة ودمتم بؤد

الخطوة الرابعة

تفعيل بروتوكول ال SSH

يقع أكثر من سبعين بالمئة من مهندسي ومديري الشبكات في خطأ فادح وهو استخدام التلنت للاتصال مع الروتر، فكما نعلم أن أغلب الأجهزة وان لم يكن كلها يحتاج منا الاتصال بها عن بعد للأطلاع عليها وعمل بعض الإعدادات لذلك يلجأ الأغلبية إلى تفعيل بروتوكول التلنت لهذه المهمة وهو أحد أكثر الأخطاء شيوعا لأن التلنت ببساطة لايقوم بتشفير اي شيء أثناء الأرسال والاستقبال ومن بينها كلمة السر والأوامر والذي يجعلها عرضة لأي عملية تجسس لذلك خطوتك الرابعة هي تفعيل بروتوكول ال SSH عوضا عن التلنت والذي يعرف بانه يقوم بتشفير عملية الاتصال بشكل كامل والإعدادات على الشكل التالي :

```
Router(config)# ip domain-name My Domain
Router(config)# crypto key generate rsa
Router(config)# line vty 0 4
Router(config-line)# login
Router(config-line)# password your password
Router(config-line)# transport input ssh
```


Mikrotik Router OS

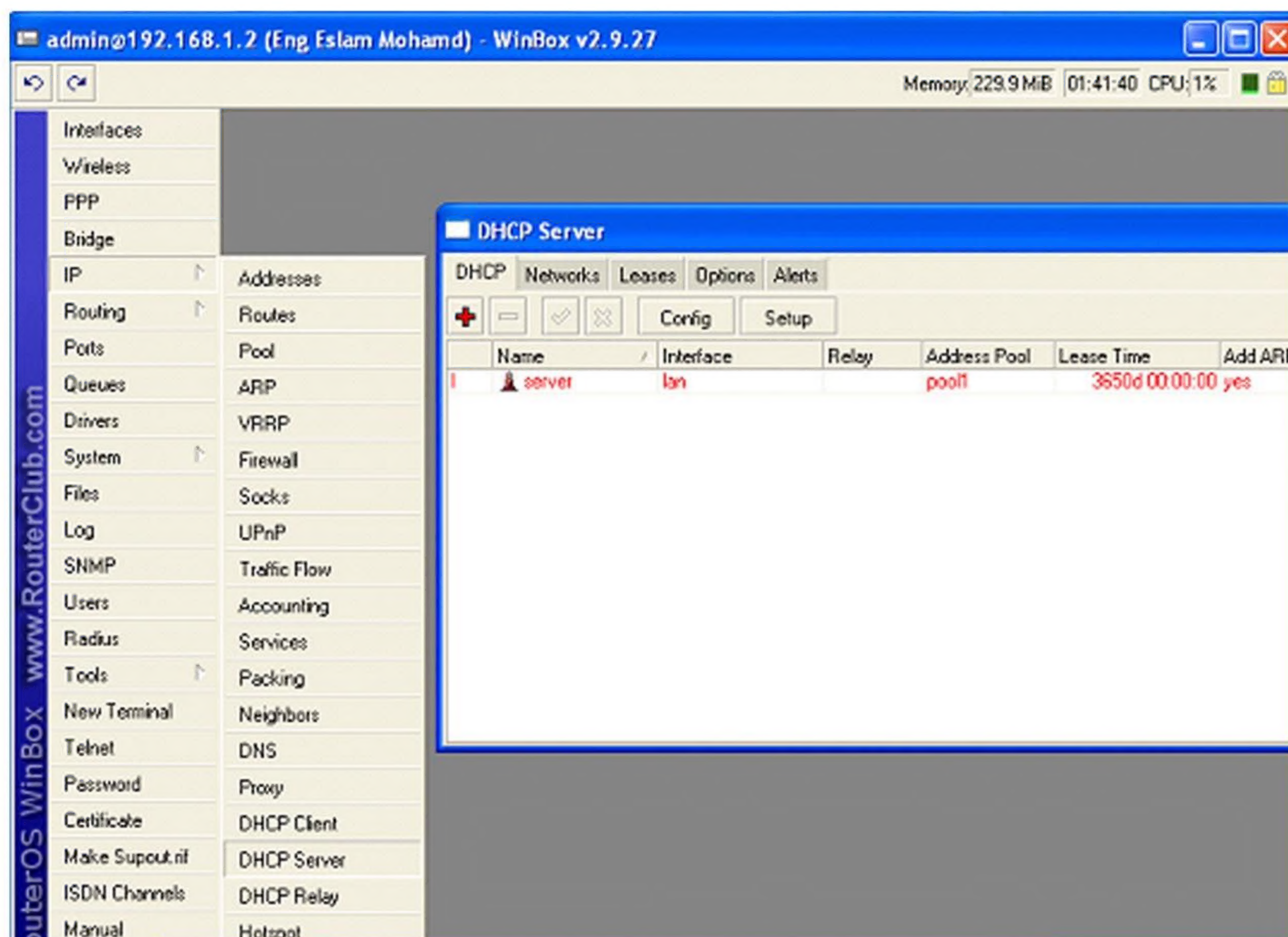
لا اعرف كيف ابداء الكلام او من اين حيث ان الكل يعرف الاحداث التى مرت بها مصر ومازلت تمر بها وموضوع الانترنت والاتصالات التى تم قطعهما بالكامل وعزلنا عن العالم كله وكنا فى داخل زجاجة وهو السبب الرئيسى فى تاخير استكمال المقالات فكل المصريون وانا اولهم نمر باصعب الظروف التى لم تستطع اقوى اجهزة المخابرات والامن فى العالم كله التنبؤ بها وهانحن الان نحاول ان نخرج من عنق الزجاجة...

Eng. Eslam Mohamed

عند قطع الانترنت لم يكن هناك اى وسيلة اتصال بالانترنت الا من خلال (الفاكس مودم) وهى الثغرة التى لم يكن يعرفها الكثير من الناس او حتى يتوقعها متخذى القرار ولكن ماهو دور المايكروتك ؟!! لقد قام البعض باستخدام خط التليفون الارضى كخط بديل لخط الانترنت اى هو البديل للكبل القادم من الروتر وتم ادخاله على المايكروتك ليقوم هو الاخر بجانبه بمعالجه الترافيك واخراجه الى العملاء مع اعاده توزيع الاشاره او الترافيك القادم من النت طبعا هذا كان الحل الوحيد فى ظل عدم وجود الانترنت والكل يعلم طبعا مدى البطى الخاص بسرعه الفاكس مودم ولكن لم يكن لدينا اى خيار اخر وهكذا وقف المايكروتك بجانب الشعب المصرى .

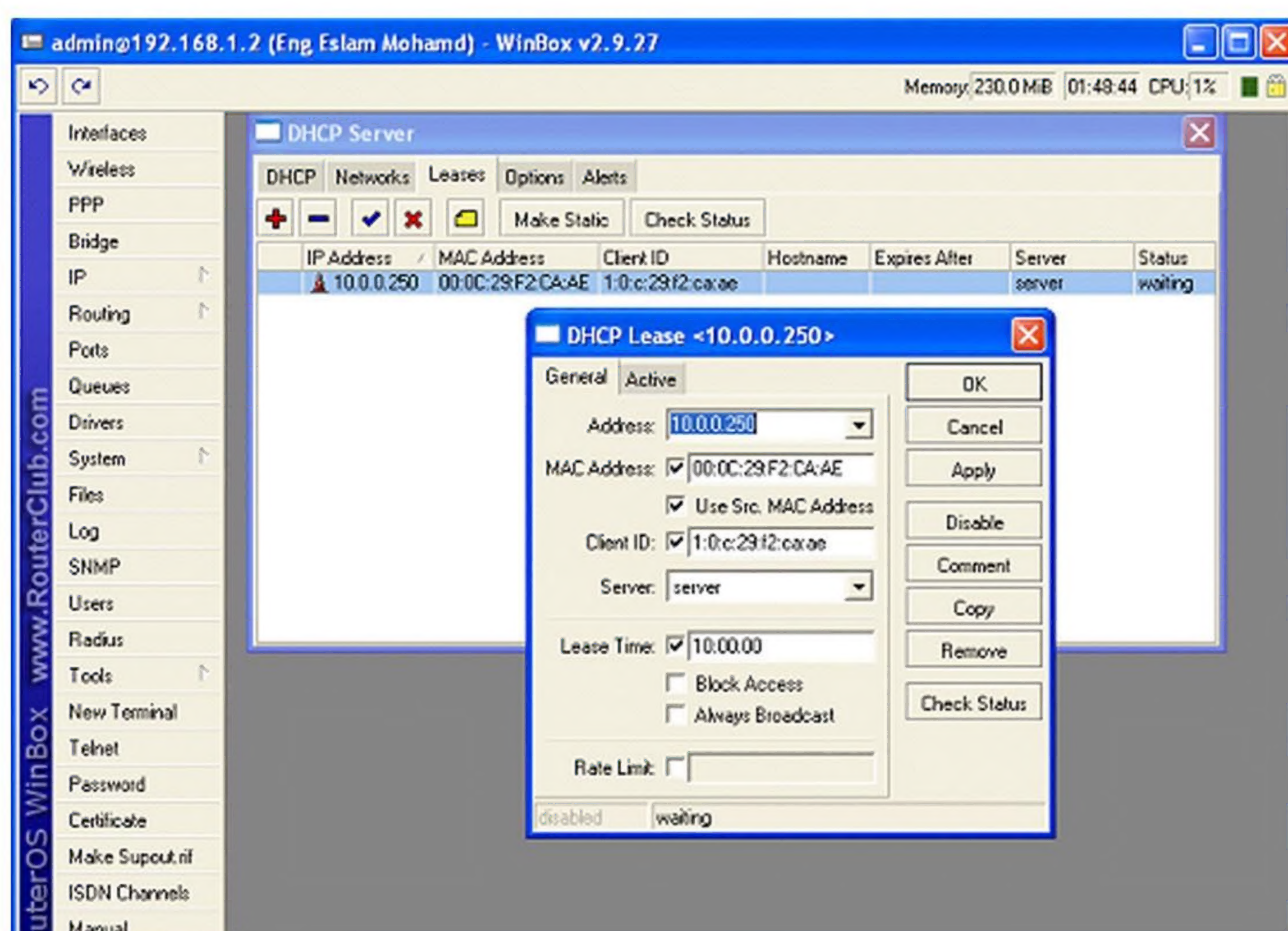
اليوم سوف نستكمل معا الموضوع الذى بدناه عن المايكروتك ولكن اليوم اود ان اقول لكم ان المايكروتك كان يعيش مع المصريين فى الاحداث الحالية !!!!!!! طبعا الكل يتسال الان كيف هذا ؟؟؟!! نعم ان المايكروتك كان له دورا كبيرا اثناء انقطاع الانترنت حيث ان الانترنت كان يعمل فقط من خلال التليفون الارضى او مايعرف بخدمه الديل اب (Dial up) والذى قد اختفى منذ زمن بعيد ولم يبق اى كروت (فاكس مودم) موجوده بالاسواق او حتى البيوت الا عند القليل من البعض والذين لم يقومون بتحديث اجهزتهم او مازلوا يحتفظون بها .

دعونا الان نتطرق لاهم ميزة فى المايكروتك بل الالهة لى شخص مهتم بمجال الاى تى او تكنولوجيا المعلومات الا وهى ال Authentication , اولا تعريف هذه الكلمة هى باختصار شديد تعنى الحقوق التى يتم السماح بها او الصلاحيات المخصصة لكل شخص وبكلام آخر هل هذا الشخص له الحق فى الدخول على الانترنت مثلا ام ليس له الصلاحيه واذا كانت له هذه الصلاحيه هل له الحق فى الدخول على كل المواقع ام هناك مواقع محجوبه او اننا نريد فقط ان يدخل هذا الشخص على مواقع معينه فقط , كل هذه الاشياء تسمى Authentication او صلاحيات .



ان المايكروتك يسمح لنا باختيار الاسلوب الذى من خلاله نعطى الصلاحيات او نقرر من هم الاشخاص المسوح لهم بالدخول على الانترنت او حتى الشبكة اولى هذه الطرق اننا يمكن ان نقوم بتفعيل ال DHCP SERVER تلك السيرفر التى تقوم بتوزيع الايبيهاات بشكل اتوماتيكى وعشوائى على المستخدمين

ولكن اذا تمكنا من معرفه الماك ادرس MAC لكل العملاء بالشبكة فيمكننا ربط الاى بي الخاص بكل عميل الذى يقوم بتوزيعه ال DHCP SERVER بالماك ادرس وبالتالي فان الكلاينت عندما يقوم بتشغيل الجهاز سوف يقوم بعمل Broadcast على الشبكة لمعرفة ال DHCP SERVER ثم يقوم بطلب الاى بي منه فان السرفر هنا يتأكد اولاً من الماك ادرس الخاص بكارتته الانترنت عند الكلاينت فاذا كان هو نفس الماك الموجود بالسرفر يقوم حينها باعطاء الاى بي الذى قمنا بتحديدده , طبعاً هذه ميزة قوية جداً حيث اننا اجبرنا العميل على اخذ اى بي معين وكأنه اى بي ثابت (static ip) وليس اتوماتيك (dynamic ip) رغم انه لم يقوم بنفسه بكتابه الاى بي على جهازه وليس هذا فقط بل اننا يمكن ان نجعل هذا العميل يحتفظ بهذا الاى بي لاي فتره نريدها مهما كانت حتى نقوم نحن بالتعديل بها بعد ذلك وهنا نكون قد منعنا مشكله الكونفليك فى الاى بي ومشكله المثلث الاصفر ...



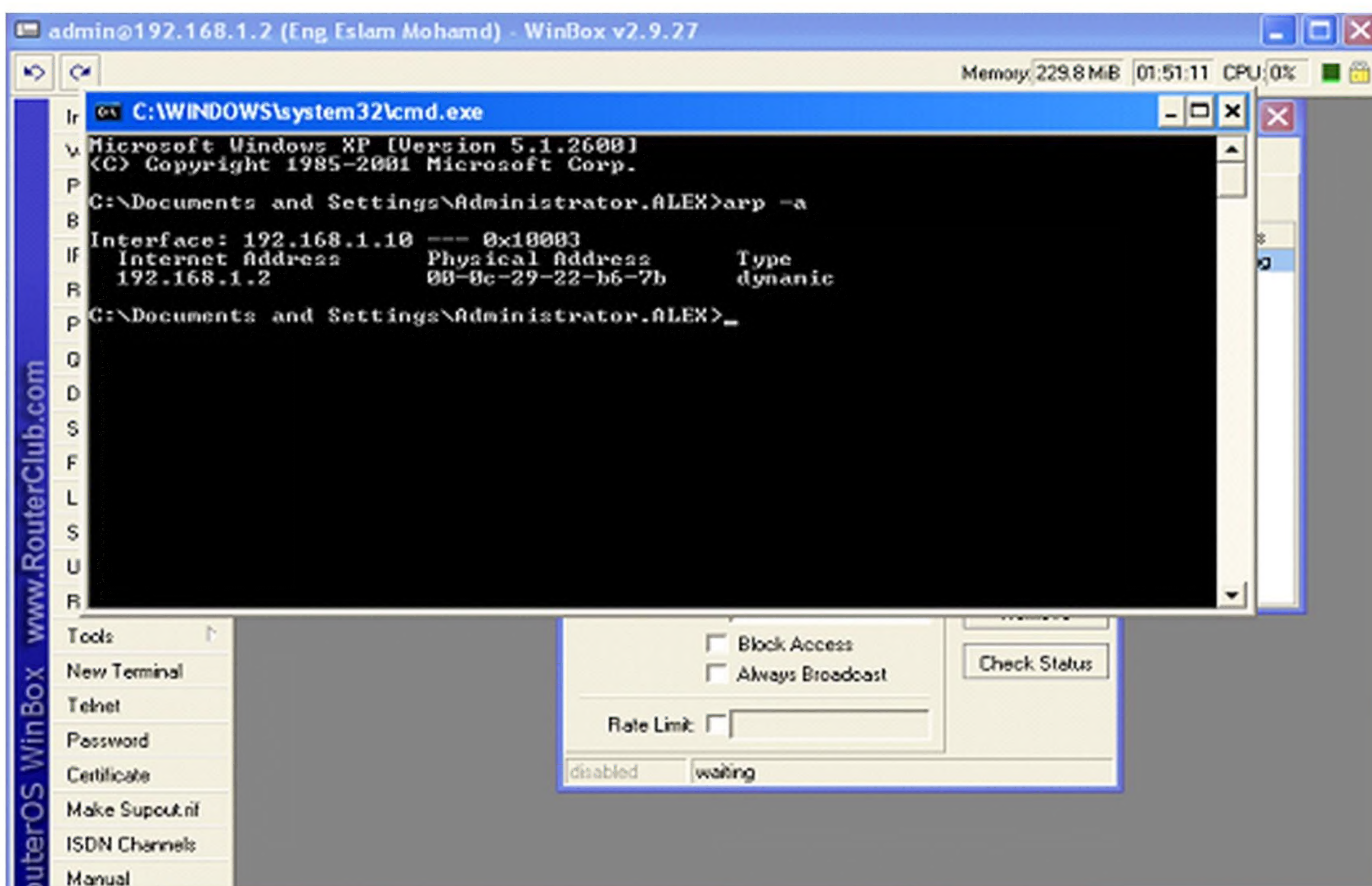
هناك سؤال الآن قد يأتى ببال البعض ماذا لو لم يكن الماك ادرس معنا هل سوف ياخذ الكلاينت اى بي ويتصل من خلال السرفر فالحقيقه نعم ولكن يمكننا ايضا التغلب على هذه المشكله بكل ببساطه حيث ان لكل جهاز مربوط بالسرفر هناك ما يسمى بجدول الارب كاش Arp وهو جدول موجود بالسيرفر حيث ان اى عميل يقوم باخذ اى بي يكون امامه الماك ادرس الخاص به كما يمكن مشاهدته هذا الجدول من الاتى

ندخل على cmd ---- run ---- stat ---- ومنها نقوم بعمل بينج على اى بي موجود معنا فى الشبكة او الجيت واى الموجود وليكم على الشكل التالى ping 192.168.1.254 بحيث تكون هناك استجابته ثم نقوم بكتابه الامر التالى arp -a لنلاحظ وجود الاى بي وامامه الماك ادرس الخاص به

ومن هنا اذا كان الاى بي صحيح بما انه اخذ من السيرفر DHCP SERVER والماك صحيح يتم الولوج الى السيرفر وانشاء الاتصال والدخول على الانترنت ولكن اذا كان الماك غير صحيح لن يتم ذلك وهو ما سوف نقوم بعمله على السيرفر حيث اننا سوف نقوم بملئ الجدول الخاص بالارب بشكل يدوى حيث سوف نقوم باضافه كل الرنجات التى

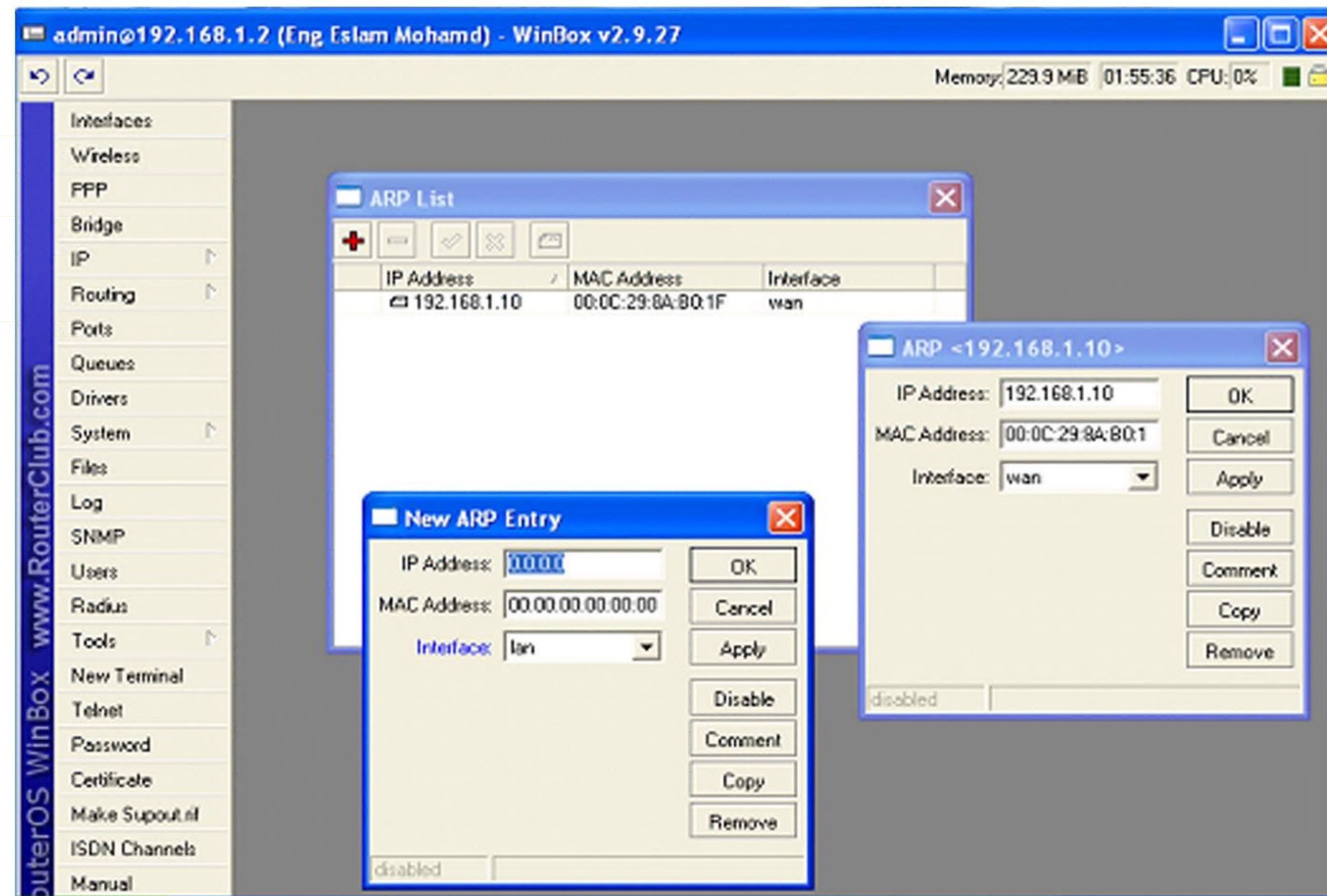
يقوم DHCP SERVER

بتوزيعها وربطها بماك ادرس غير صحيح او اصفار كما يقوم البعض



Mikrotik Router OS

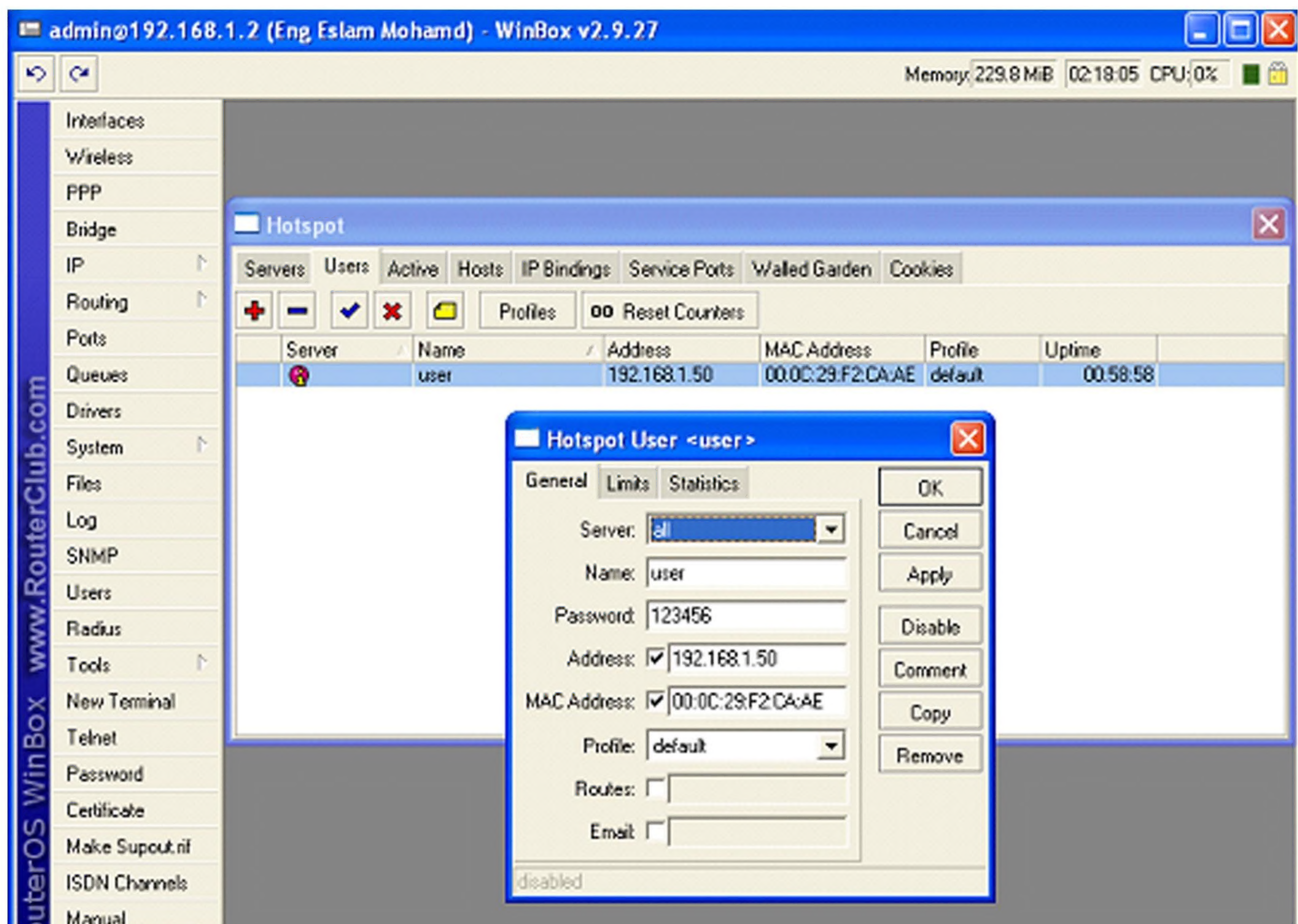
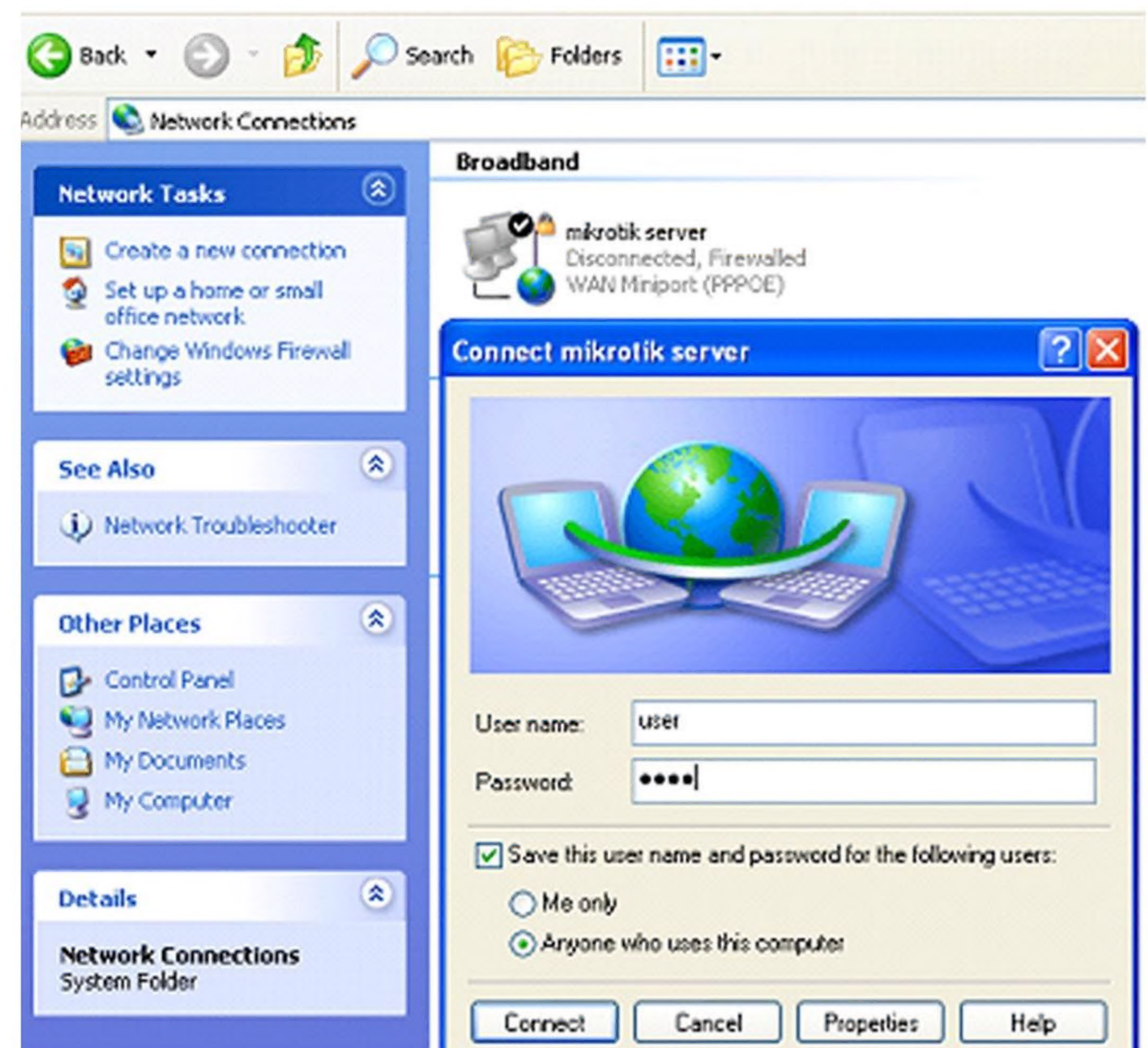
وعندها الكلينت سوف يحصل على اى بى لكن الماك غير صحيح فهو غير مطابق للماك الموجود بالسرفر حينها سوف لن يتم الاتصال وهى احدى اساليب الحماية الموجود بالمايكروتك.



ايضا من هذه الطرق ان تكون ال Authentication من خلال يوزر نيم وباسورد وهدى الطرق للذين يقومون باستخدام طريقه ال hotspot فى الاتصال او pppoe وهى الطرق التى يتم من خلالها ادخال اسم مستخدم وكلمه سر اما فى شاشه لوجن او صفحه متصفح html كما نلاحظ من الصور



وهي من بعض السيرفرات حيث ان عملية Authentication تتم من خلال اسم مستخدم وكلمه سر , وليس ذلك فقط بل اننا يمكننا التحكم في الكلاينت صاحب كلمه السر بمعنى هل من الممكن ان يستخدم كلمه السر واسم المستخدم من اي جهاز على الشبكة ام من على جهاز معين حيث ايضا يمكن ربط الاي بي او الماك ادرس او الاثنين معا باسم المستخدم وكلمه السر



نكتفي اليوم بهذا القدر وعلى وعد باستكمال باقى الحلقات فى الاعداد القادمه باذن لله
لنتعرف اكثر على اهم الخدمات التى يقدمها المايكروتك

عادة

عندما نبدأ تصفح المواقع
تبدأ العملية من خلال كتابة
أسم الموقع أولا ولكن مثلا موقع
networkset.net نجد أن الموقع قد فتح
ومن دون ان نشعر بأي شيء حدث.

وحقيقة عملية طلب الموقع تمر بمرحلة خفية تجري بدون ان
نشعر بها وهي عملية الـ DNS Resolving تقوم هذه العملية
ببساطة على ترجمة اسم الموقع networkset.net إلى الأيبي
وطبعا هذه العملية مهمة كوننا نعلم أن كل ما يجري من خلال
الشبكات يتم من خلال الأرقام فقط وليس العنوان وتعتمد هذه
الاجهزة في عملية الترجمة على سيرفرات تعرف بي DNS أو

Domain Name Server وما قد لانعرفه

أيضا أن عمليات الترجمة هذه تحفظ في

جداول مؤقتة في ذاكرة الجهاز وتنزل مع أول
عملية إعادة أغلاق للجهاز وهي مهمة حتى يعود
لها الجهاز مرة أخرى لو في حال طلب مستخدم
الجهاز الموقع ذاته.

لنلقي نظرة أكثر قربا على كيفية تحليل العناوين
عندما نقوم بطلب اسم موقع فإن أول خطوة
تتم هي عملية تحليل العنوان وذلك بالبحث في
الجدول الموجود في الـ resolver والذي يضم
اسماء وعناوين المواقع التي تم فتحها مؤخرا ، كما
في الصورة المجاورة :

DNS cache poisoning

صفحة الرمزاني

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Safa>ipconfig /displaydns

Windows IP Configuration

api.yontoo.com
-----
Record Name . . . . . : api.yontoo.com
Record Type . . . . . : 1
Time To Live . . . . . : 729
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 38.107.189.4

www.google.com
-----
Record Name . . . . . : www.google.com
Record Type . . . . . : 5
Time To Live . . . . . : 90
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : www.l.google.com
```


الهجوم

هناك عدة اسباب تجعل المهاجمين يقومون بشن هجماتهم على الـ DNS server سأذكر الاسباب الرئيسية لمثل هذه الهجمات :

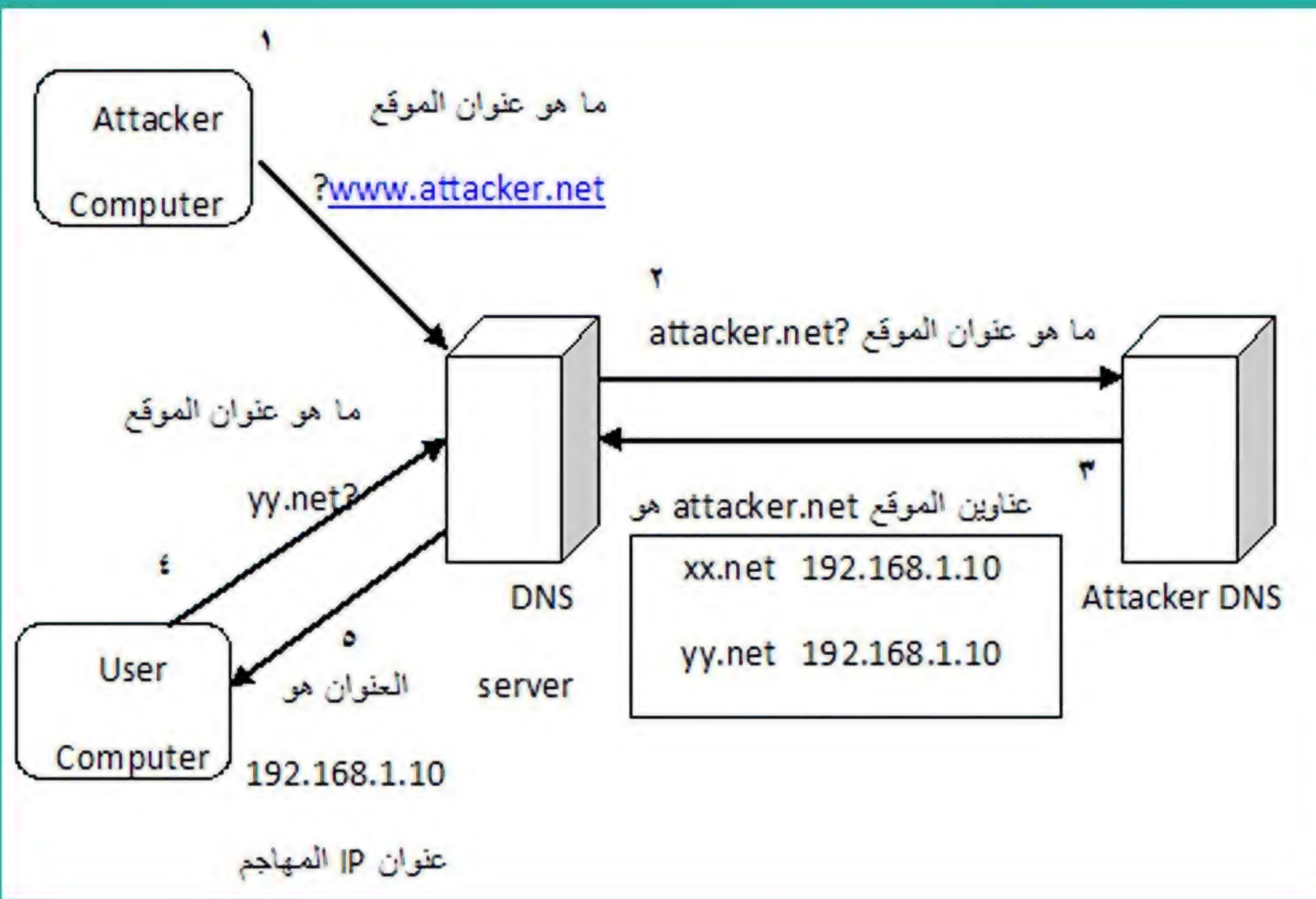
1_ سرقة الهوية identity theft

2_ نشر الـ malware

3_ نشر معلومات خاطئة ومغلوبة

4_ السبب الرابع هو ما يعرف بهجمات man_in_the_middle .

فكرة الهجوم تقوم على تبديل وتزوير عنوان الموقع ، فمثلا لو قام المستخدم بطلب عنوان الموقع good.com والذي عنوانه 203.193.14.103 فإن الهجوم سيتسبب بإرجاع العنوان 209.186.22.90 والذي هو عنوان موقع المهاجم . والشكل المجاور يوضح آلية الهجوم :



(نلاحظ ان الـ Attacker DNS server قد يعيد نفس العنوان لأكثر من موقع وكلما تم طلب احد هذه المواقع سيتم اعادة العنوان المزور وبالتالي سيزداد عدد الضحايا) .

عندما يستلم الـ local DNS الرد من سيرفر المهاجم (الذي يظهر ويدعي انه السيرفر الموثوق) فإن عنوان الـ IP مع اسماء المواقع سيتم حفظهم في الـ local DNS cache ومن ثم يرسل العنوان إلى الـ local DNS resolver وبالتالي سيكون كل من الـ local DNS والـ resolver مصابين ، فعندما يقوم اي جهاز في هذه الشبكة بطلب هذا الموقع فإن الـ DNS server سيقوم بإرسال عنوان موقع المهاجم ، وهكذا تبقى الإصابة إلى ان تنتهي فترة الـ Time to live الخاصة بهذا الموقع فيتم حذف العنوان من الجدول او الـ cache .

فإذا وجد عنوان الموقع فسيعيد النتيجة أما إذا لم يجده في الجدول فإن الـ DNS resolver سيقوم بإرسال طلب إلى الـ local DNS والذي بدوره يقوم بالبحث عن العنوان في الـ cache الموجود فيه فإذا وجد النتيجة سيقوم بإرسالها إلى الـ DNS resolver أما إن لم يجده في الـ cache فإنه يقوم بإرسال الطلب إلى الـ root DNS وهكذا إلى أن يحصل على رد بعنوان الموقع المطلوب وبالتالي فإن الـ local DNS سيقوم بحفظ اسم الموقع وعنوانه في الـ cache الخاص به ومن ثم إرسال اجابة لـ DNS resolver بعنوان الموقع ، والأخير سيقوم بحفظ العنوان في الجدول الخاص به والاتصال بالموقع المطلوب من خلال عنوانه .

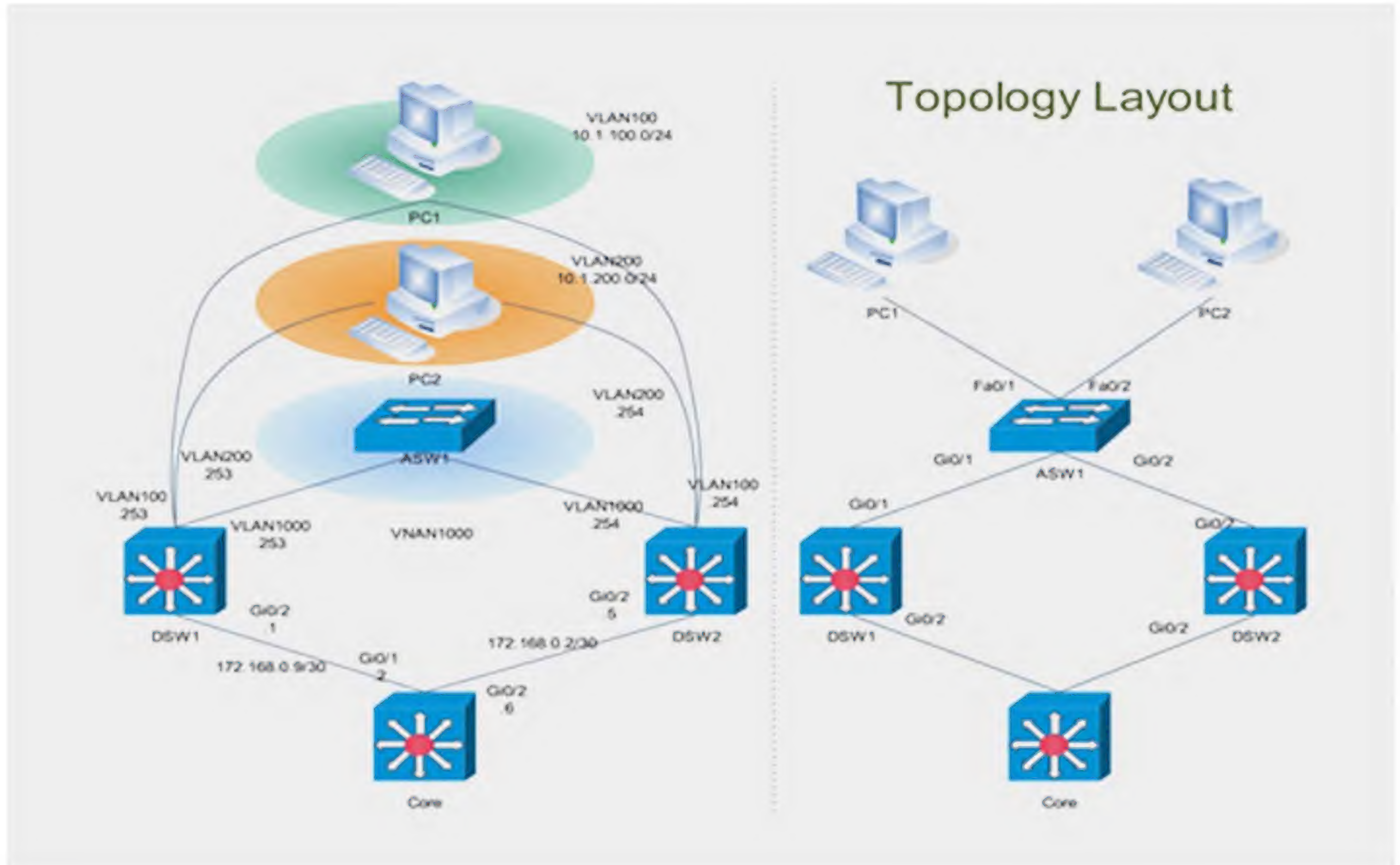
(في حال عدم الحصول على عنوان الموقع فهذا يعني أن الموقع غير موجود على شبكة الانترنت) .

الحماية

هناك عدة امور تقلل من خطر هذه الهجمات ، فمثلا استخدام احدث اصدارات برامج الـ DNS مثل برامج الـ BIND والـ DNSSEC (Domain Name Security Extensions) والذي يعد افضل من سابقه وأقوى وأكثر أمانا (حيث ان هذه البرامج تقوم بعمل فلتر للردود المستلمة ورفض اي عناوين اضافية وتتبع أليات متطورة في عملية ارسال واستقبال الاستفسارات) ، وايضا من طرق تقليل الهجوم فصل الـ external DNS server عن الـ internal DNS server ، والتأكد من موثوقية ومصداقية السيرفر الذي يرسل الإجابة ، وكذلك إخفاء رقم اصدار البرامج المستخدمة يساعد على تخفيف الهجمات ، وإزالة الخدمات غير الضرورية من الـ DNS server ، ويفضل استخدام البرامج احادية المهمة عن البرامج متعددة المهام .

اسأل الله أن أكون وفقت في الطرئ ، وإن أصبت فمن الله وإن أخطأت فمن نفسي ، والسلام عليكم ورحمة الله وبركاته .

مقالتي لهذا العدد سوف تتحدث عن أفضل البرنامج المعتمدة للقيام بعمل مخططات أو Diagram للشبكة من أجل توثيقها والأطلاع عليها وقت الحاجة لان وجودها يعتبر أحد أهم الأشياء التي تساعد مدير الشبكة على فهم الشبكة التي لديه وكيف تعمل والتي يلجأ لها دائما لحل أي مشكلة تواجهه في الشبكة لأنها ببساطة تقدم له كل المعلومات اللازمة لبدأ عملية ال Troubleshooting على الشبكة.



البرنامج الأول

Edraw Network Diagram 5.2

شهرة هذا البرنامج لاتقل عن شهرة البرنامج الأول وأمكانياته كثيرة أيضا في مجال الشبكات وهو أيضا برنامج غير مجاني وثمانه 69 دولار ومن مميزاته الجميلة امكانية عمل مخطط بشكل ثلاثي الأبعاد بالإضافة إلى دعمه للأجهزة الخاصة بسيسكو وهذه صورة توضيحية

بالنسبة لي تعاملت مع هذا البرنامج أكثر من الأول وأعجبتني أكثر البرنامج يأتي تجريبي ولمدة 30 يوم تستطيع تحميله من موقع البرنامج على الرابط التالي:

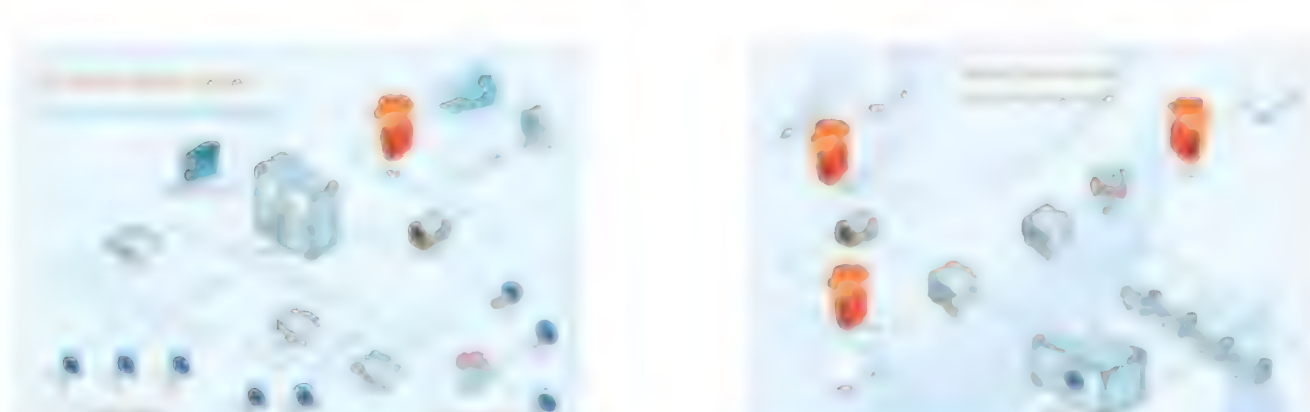
<http://www.edrawsoft.com/download.php>

للقسم المخصص للشبكات .

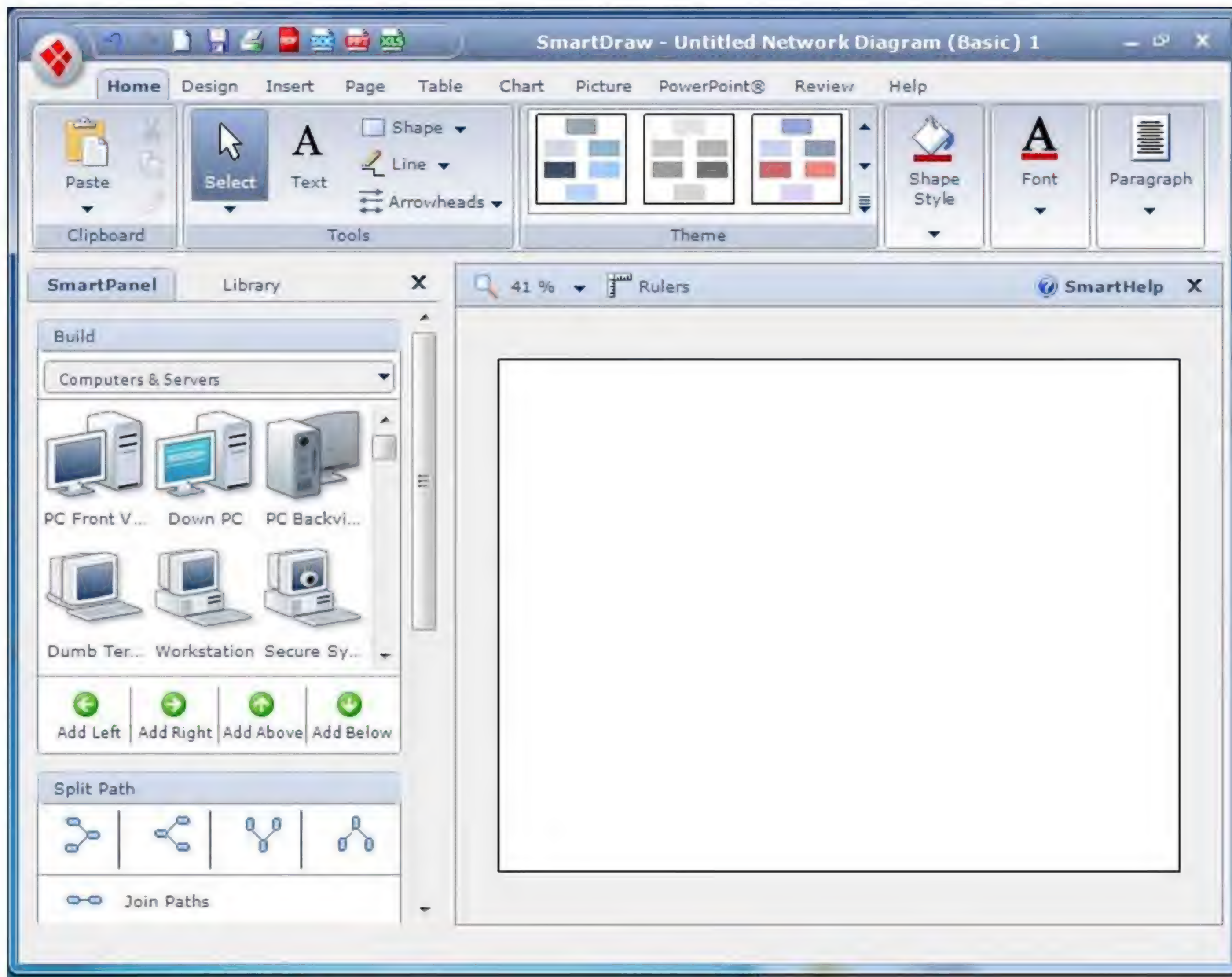
Templates



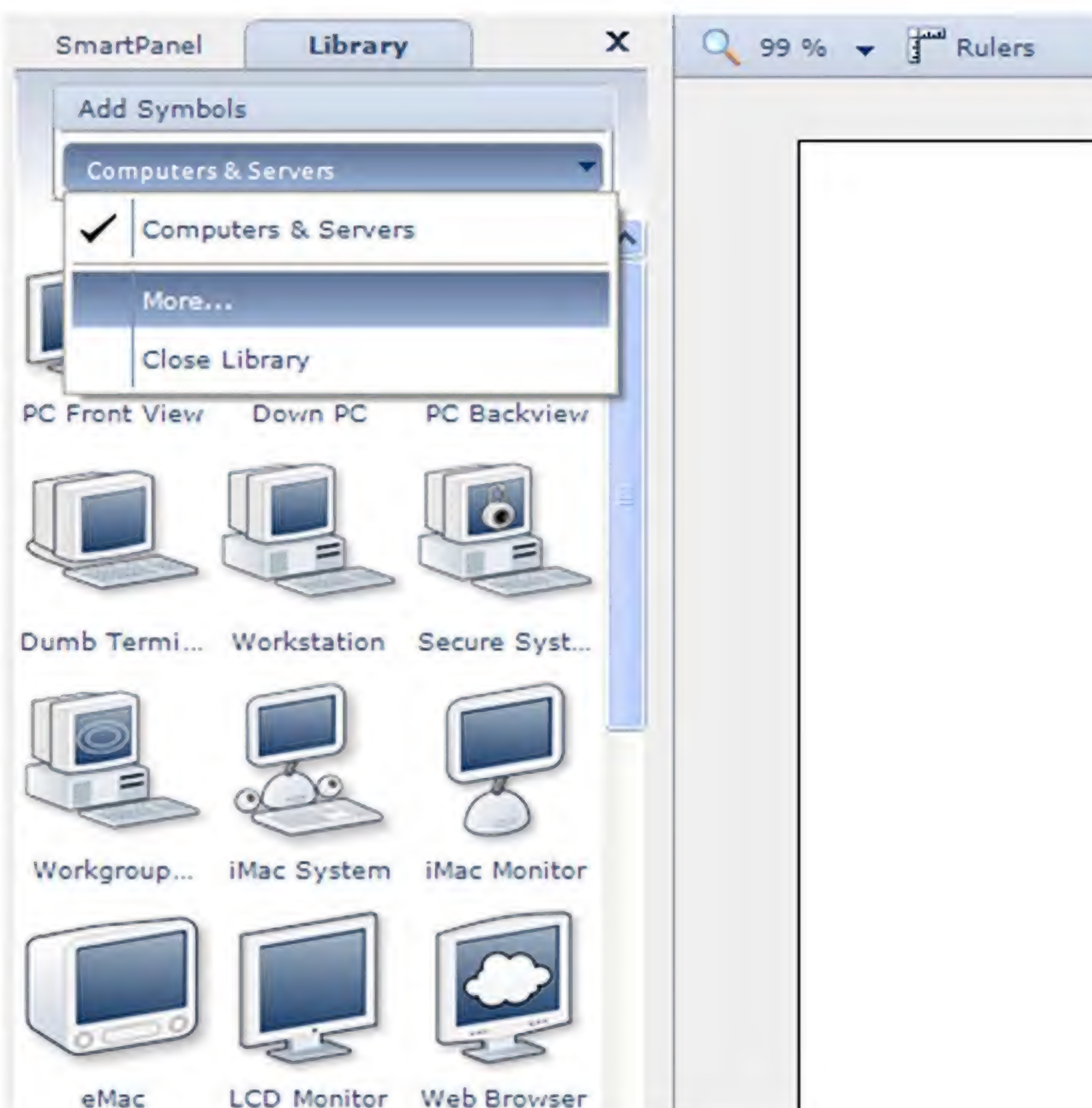
Examples www.networkset.net



المهم مايلزمنا من كل هذه الخيارات هو الأيقونة المظلة والخاصة بالشبكات نقوم بالضغط عليها لنبدأ رسم المخطط الذي نريده وسوف تصادفنا هذه الصورة



ونبدأ تصميم الشبكة بالأيقونات المتاحة وأحب أن أضيف أن مع البرنامج هناك عدد كبير جداً من الأيقونات والتي تستطيع الوصول لها من خلال الضغط على زر المكتبة Library وبعدها تابع معي بالصورة



البرنامج الثاني

SmartDraw 2010

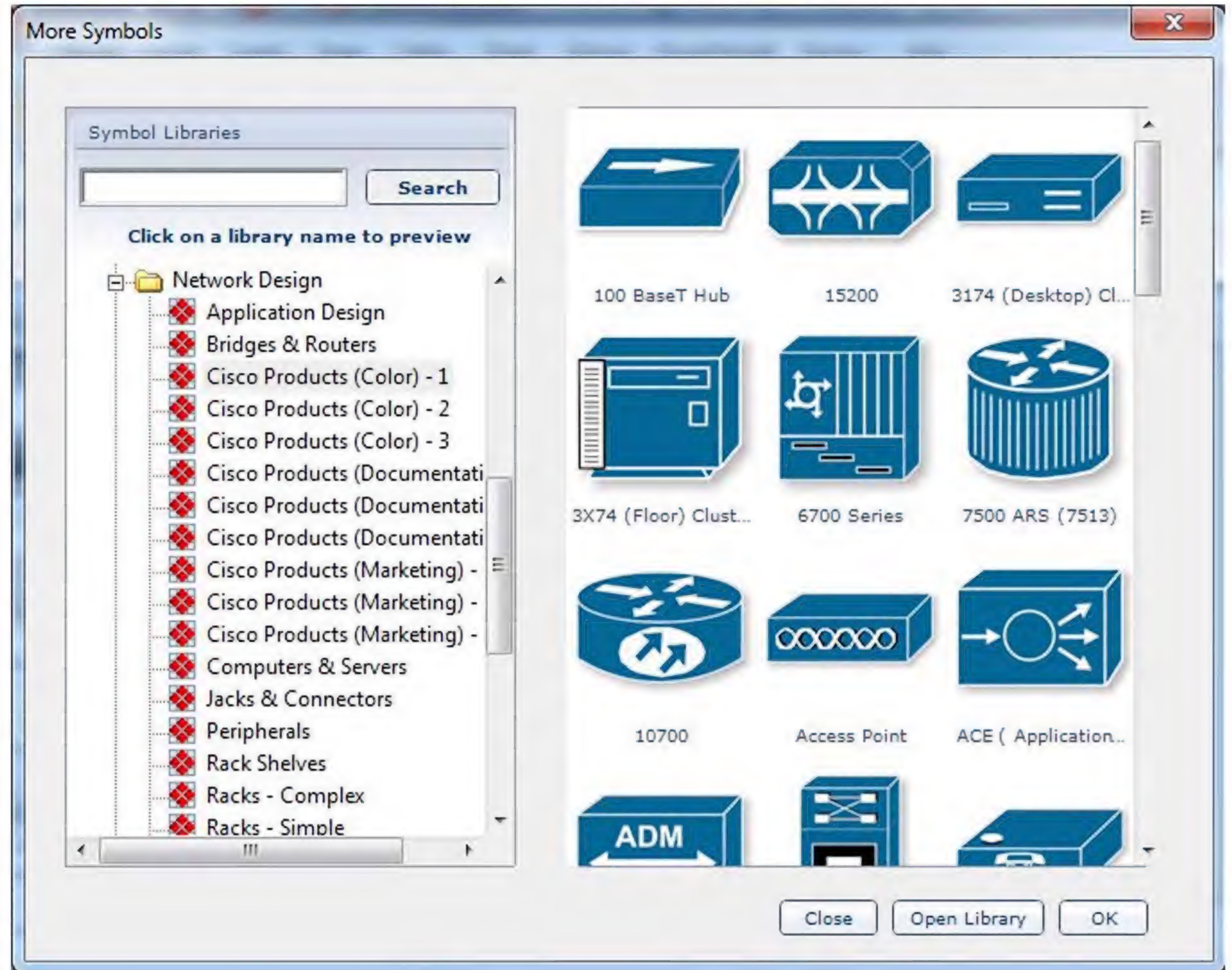
أحد أشهر وأفضل البرامج الموجودة في هذا المضمرة وهو برنامج غير مجاني وثمانه 179 دولار وهو برنامج ضخم جداً بأمكانياته فهو يتيح لك عمل رسومات ومخططات للعديد من الأشياء وليس فقط للشبكات بالإضافة إلى إمكانية حفظ المخطط على شكل صورة أو ملف PDF أو HTML أو للأوتوكاد وهذه صورة توضيحية لأمكانيات البرنامج .



وعندها سوف تحتاج لك كمية كبيرة جدا من الأيقونات لرسم المخطط الذي تريده وخصوصا الأيقونات الخاصة بأجهزة سيسكو و يمكنك تجربة البرنامج لسبعة أيام فقط وهذا رابط تحميل البرنامج :

http://download.cnet.com/SmartDraw-20103000/10002466-4_2075-.html

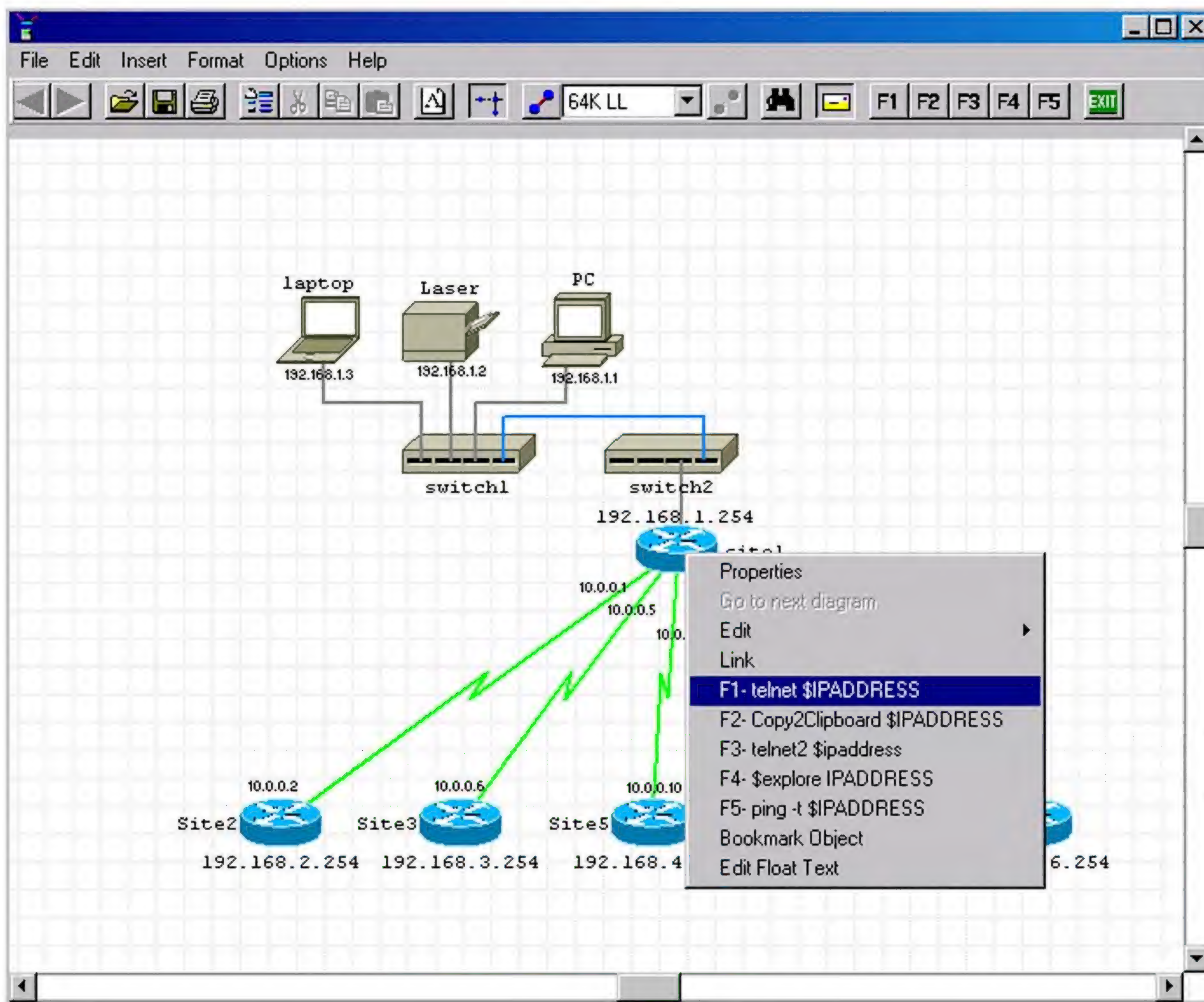
أو من موقع البرنامج الرسمي :
<http://www.smartdraw.com/downloads/>



البرنامج الثالث

Network Notepad 4.6.6

برنامج بسيط ومجاني ويمكنك ايضا من عمل مخططات للشبكة وهذه صورة توضيحية لكيفية الرسم على البرنامج



لتحميل البرنامج أتجه إلى الرابط التالي
<http://www.networknotepad.com/index.htm>

لتحميل أيقونات إضافية للبرنامج :
<http://www.networknotepad.com/library23.zip>

ولتحميل أيقونات خاصة بسيسكو :
<http://www.cisco.com/web/about/ac50/ac472/.html>

البرنامج الرابع

CuteDraw 2.0

ايضا برنامج بسيط وغير معقد وهو غير مجاني ويقوم بنفس الوظيفة بالنسبة لي لم أقم بتجربة هذا البرنامج هذه صورة توضيحية لكيفية الرسم على البرنامج .

لتحميل البرنامج وتجربته لمدة 30 يوم من موقع البرنامج الرسمي :

<http://www.cutedraw.com/download.php>

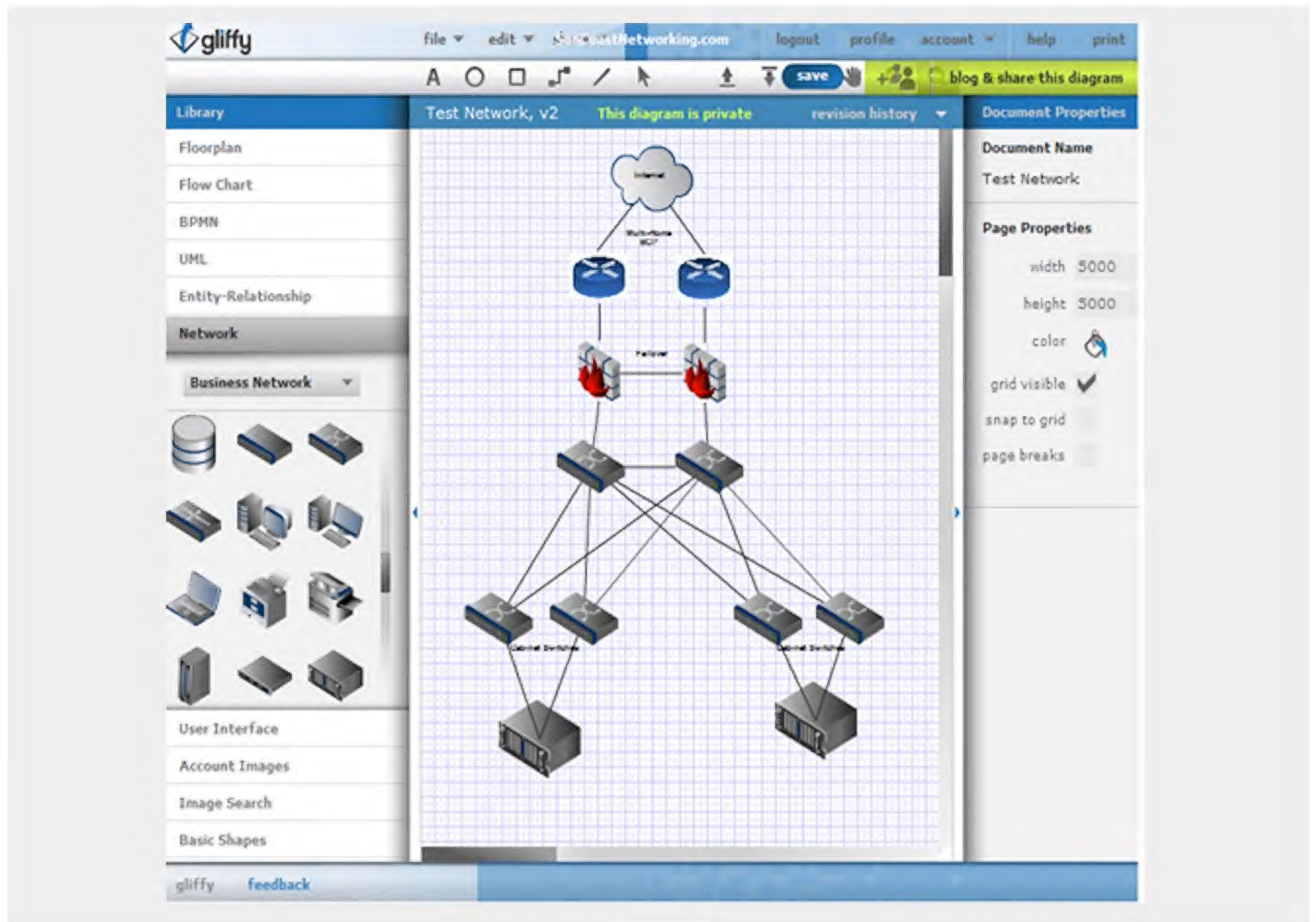
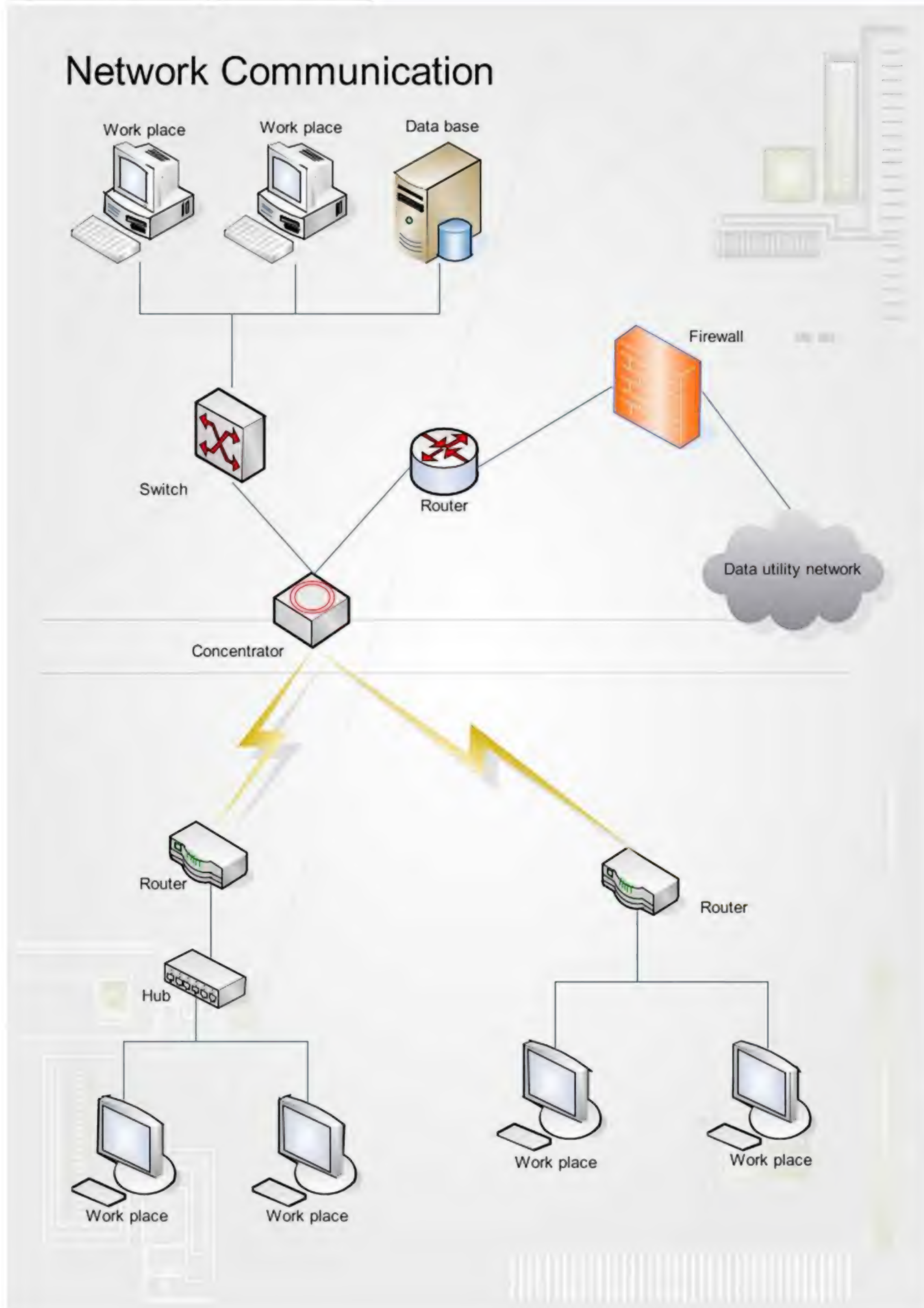
وأخيرا هناك مواقع تتيح لك عمل مخططات on line وبدون الحاجة لتحميل أي برنامج وهي تعمل تحت تقنية الـ Cloud Computing التي سوف تحدث عنها الأستاذ ياسر رمزي في مقال سابق من المجلة .

وهذه بعض المواقع المجانية المخصصة لهذه الوظيفة :

<http://draw.labs.autodesk.com/ADDdraw/draw.html>

<http://www.gliffy.com>

وفي الأسفل صورة توضيحية لطريقة عمل مخططات على الموقع الثاني





Echo Technology

Integratoin Technical Solution

Network - Web Design

Training & Development

Programing - Design & Printing

Electronic System - Control System

**Whole Technical
One Supplire**

Study and implementation of engineering projects

Syria - DeirEzzor - Telefax: 051 218452 - Mob: 0967 96265 - 0955 478942

Website: WWW.EchoTechno.com - E-mail: Info@EchoTechno.com (Soon)

يعتبر OSI Model بطبقاته السبع نموذج نظري دراسي جميل و مرتب لطريقة عمل الشبكات بكل معداتھا و برمجياتھا و تقنياتها , و قد مر عليه أي متخصص أو مبتديء في الشبكات و درسه طلاب أقسام الكمبيوتر و الإتصالات في الجامعات

الجديد في الأمر أن يتم استخدام فهمك لهذا النموذج في صيانة الشبكة و تتبع خطائھا و وضع حلول لها أو العكس أي أن يكون طريقة صيانتك و تتبع أخطاء شبكتك وسيلة جيدة لفهم هذا النموذج

Group	#	Layer Name	Common Protocols and Technologies	Common Network Components Associated with this Layer
Upper Layers	7	Application	DNS, NFS, DHCP, SNMP, FTP, TFTP, SMTP, POP3, IMAP, HTTP, Telnet	Network aware applications, Email, Web Browsers and Servers, File Transfer, Name Resolution
	6	Presentation	SSL, Shells and Redirectors, MIME	
	5	Session	NetBIOS, Application Program Interfaces, Remote Procedure Calls	
Lower Layers	4	Transport	TCP and UDP	Video and Voice streaming mechanisms firewall filtering lists
	3	Network	IP, IPv6, IP NAT	IP Addressing, Routing
	2	Data Link	Ethernet Family, WLAN, Wi-Fi, ATM, PPP	Network Interface cards and Drivers, Network Switching, WAN connectivity
	1	Physical	Electrical Signaling, Light Wave Patterns, Radio Wave Patterns	Physical Medium (copper twisted pair, fiber optic cable, wireless transmitters), Hubs and Repeaters

دعنا نتصور هذا النموذج كطبقتين فقط كما تري في الشكل السابق إحداهما عليا وتشمل الثلاث طبقات القريبة في تعاملها مع السوفتوير و الأخرى الدنيا و تشمل الأربع طبقات القريبة في تعاملها مع الهاردوير و سنفترض الآن أننا نريد أن نطبق نظرية التعامل بطبقات الشبكة في معرفة سبب انقطاع الإنترنت عن جهاز ما و هي أبسط المشاكل و أكثرها شيوعا و حيث أن المشكلة تخص الإنترنت فسنقوم بتبسيط نموذج OSI الى نموذج TCP/IP و كل ما علينا فعله أن نقوم بضم الثلاث طبقات العليا Application , Presentation , Session في طبقة واحدة و نتعامل معها على هذا الأساس

و لكل مهندس طريقته في بدء التعامل مع هذا النظام فمنهم من يبدأ من الأعلى و منهم من يبدأ بالأسفل و غالبا ما تكون طبيعة المشكلة هي التي تحتم علي مسئول الصيانة من أين يبدأ و سنقوم في كل طبقة بسؤال أنفسنا بعض الأسئلة منها و أهمها و أكثرها شيوعا هو ما تراه في الشكل التالي ثم نجيب عليها و من ثم نقترح الحل و ذلك في حدود المشكلة التي عرضناها و هي انقطاع الإنترنت عن جهاز في شبكة ما



نادر الهنسي

و تتمثل إحدى مشكلات هذه الطبقة في مشاكل تخص الطاقة الكهربائية مثل انفصال الكهرباء خارج الجهاز Device power off أو داخله مثل Power supply أو فشل أحد الشرائح الإلكترونية داخل الجهاز أو بالنسبة لمشكلتنا فإن غالب الأمر أنها تخص كابلات الشبكة فلا تعمل كليا Faulty network cable أو استخدام كابل خاطيء Incorrect cable type

Layer 2 Troubleshooting

Layer 3: Network

هل تستطيع الإتصال بالراوتر أو gateway الذي يصلك بالإنترنت

الجهاز أيضا الي الآن لا يستطيع الإتصال بالإنترنت رغم تغلبنا علي مشكلات الطبقة الأولى و الثانية في هذه الطبقة و التي تسمى بالطبقة الثالثة أو طبقة الشبكة Network تقع عدة بروتوكولات أهمها بروتوكولات التوجيه Routing و بروتوكول IP , و في حال استخدامك راوتر في شبكتك و قمت بإعدادة و ضبط بروتوكولات التوجيه به فإنه يجب عليك حينها أن تتأكد من سلامة عمل هذه البروتوكولات و هذه الجزئية فقط هي أحد المحاور الرئيسية في منهج سيسكو الجديد TSHOOT ضمن حزمة CCNP الجديدة أما IP فهو كلمة السر الرئيسية في هذه الطبقة و ما يتعلق به من أقنعة الشبكة و البروتوكولات المساندة مثل DHCP و IP هنا قد يكون عنوان الجهاز الشبكي أو عنوان بوابة الإنترنت gateway أو ربما يكون عنوان DNS IP أو عنوان Proxy IP و تكمن المشكلة في عدم قدرة الجهاز من رؤية الأجهزة الأخرى في نفس الشبكة رغم اتصالها عمليا و ماديا و تكون عدم القدرة علي الإتصال ناشئة عن عدم وجود هذه العناوين أصلا أو فقدان القدرة علي الإتصال بسيرفر DHCP و الذي يقوم أوتوماتيكيا بحجز هذه العناوين لكل جهاز و لدينا عدة أدوات للكشف عن هذه الأخطاء

Layer 5-7: Upper Layers

هل تستطيع الإتصال بالإنترنت بواسطة المتصفح أو أي برمجيات أخرى

Layer 4: Transport

هل لديك جدران نارية Firewall علي جهازك أو تستخدمه في شبكتك

Layer 3: Network

هل تستطيع الإتصال بالراوتر أو gateway الذي يصلك بالإنترنت

Layer 2: Data Link

هل تأكدت من عمل كارت الشبكة NIC علي جهازك

Layer 1: Physical

حاول أن تتأكد من عمل الكابلات التي تصل الأجهزة بالسويتش أو السويتش بالراوتر

هيا نبدأ العمل و سنأخذ الطريق من الأسفل الي الأعلى

Layer 1 Troubleshooting

Layer 1: Physical

حاول أن تتأكد من عمل الكابلات التي تصل الأجهزة بالسويتش أو السويتش بالراوتر

طبقا لفهمك لهذه الطبقة – و التي يسمونها الفيزيائية طبقا للترجمة الحرفية و أحب أنا أن اسميها الطبقة المادية – فأنت تعلم انها تختص بالهاردوير أي الشيء الملموس من الكمبيوتر أو الشبكة سواء كان ميكانيكيا أو إلكترونيا أو كهربيا أو معماريا أو بشكل أصح هي الطبقة التي ان حدثت فيها مشكلة فإنك تستطيع تمييزها بالحواس الخمس أي تستطيع أن تراها او تشمها و تلمسها و تشمها بل و تتذوقها أيضا فما بين الملاحظة بالعين عدم وجود فلاش ضوء بعض الأجهزة الي سماع بالأذن اصوات اضطرابات في المراوح و مرورا بالإحساس باللمس بسخونة جزء معين من الهاردوير نهاية الي شم بالأنف شبه اشتعال او احتراق احدي الرقائق الإلكترونية في الجهاز




```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\nader>ipconfig

Windows IP Configuration

PPP adapter Zain 3G:

    Connection-specific DNS Suffix . : 
    IPv4 Address. . . . . : 10.183.137.164
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 0.0.0.0

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::952d:cfa0:e2b1:cb5f%11
    IPv4 Address. . . . . : 192.168.190.111
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.190.1
```

ipconfig : يبين إعدادات IP في الجهاز و هنا نتأكد من وجود العناوين الخاصة بالجهاز و سلامة قناع الشبكة subnet mask و كذلك من وجود عنوان بوابة الإنترنت أو الراوتر Gateway

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\nader>ping 192.168.190.3

Pinging 192.168.190.3 with 32 bytes of data:
Reply from 192.168.190.3: bytes=32 time<1ms TTL=128
Reply from 192.168.190.3: bytes=32 time<1ms TTL=128
Reply from 192.168.190.3: bytes=32 time<1ms TTL=128
Reply from 192.168.190.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.190.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\nader>ping 192.168.190.1

Pinging 192.168.190.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.190.1: bytes=32 time=1ms TTL=255
Reply from 192.168.190.1: bytes=32 time=1ms TTL=255
Reply from 192.168.190.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.190.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

السيرفر

الراوتر

ping : يختبر اتصال الجهاز بعنوان آخر خاصة السيرفر الذي يعطي خدمات DHCP أو الراوتر

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\nader>tracert 192.168.190.1

Tracing route to 192.168.190.1 over a maximum of 30 hops
  0  1 ms    1 ms    1 ms  192.168.190.1
Trace complete.

C:\Users\nader>tracert 192.168.190.3

Tracing route to LAB2900SRV [192.168.190.3]
over a maximum of 30 hops:
  0  <1 ms   <1 ms   <1 ms  LAB2900SRV [192.168.190.3]
Trace complete.

C:\Users\nader>tracert www.zain.com

Tracing route to www.zain.com [72.32.84.240]
over a maximum of 30 hops:
  0  *        *        *        Request timed out.
  1  *        *        *        Request timed out.
  2  *        *        *        Request timed out.
  3  104 ms   100 ms   119 ms   62.150.83.41
  4  128 ms   119 ms   119 ms   if-10-2-core1.RSD-Riyad.as6453.net [116.0.78.9]
  5  237 ms   229 ms   219 ms   Pos-channel1.ncore3.LDN-London.as6453.net [116.0.78.42]
  6  227 ms   217 ms   *        Ulan463.icore1.LDN-London.as6453.net [195.219.195.38]
  7  207 ms   219 ms   219 ms   xe-10-2-2.edge3.London1.level3.net [4.68.63.105]
  8  248 ms   239 ms   229 ms   ae-34-52.ebr2.London1.Level3.net [4.69.139.97]
  9  293 ms   299 ms   279 ms   ae-41-41.ebr1.NewYork1.Level3.net [4.69.137.66]
 10  277 ms   299 ms   280 ms   ae-61-61.csw1.NewYork1.Level3.net [4.69.134.66]
 11  298 ms   319 ms   *        ae-62-62.ebr2.NewYork1.Level3.net [4.69.148.33]
 12  397 ms   389 ms   389 ms   ae-3-3.ebr2.Dallas1.Level3.net [4.69.137.121]
 13  368 ms   379 ms   389 ms   ae-3-80.edge2.Dallas3.Level3.net [4.69.145.140]
 14  377 ms   389 ms   389 ms   RACKSPACE-M.edge2.Dallas3.Level3.net [4.59.36.50]
 15  397 ms   389 ms   399 ms   vlan901.core1.dfwi1.rackspace.com [72.3.128.21]
 16  377 ms   379 ms   389 ms   aggr4a.dfwi1.rackspace.net [72.3.129.15]
 17  347 ms   369 ms   399 ms   72.32.84.240
Trace complete.

C:\Users\nader>
```

الراوتر

السيرفر

موقع ما لثري استجابة الوصول اليه

tracert : التأكد من سلامة الإتصال بين الجهاز و الجهة التي يريد الإتصال بها و تتبع الخطوات المؤدية لذلك

و هناك برمجيات احترافية و متخصصة بل و مجانية أيضا تستخدم أسس هذه الأوامر و لكن بواجهة مرئية مريحة تستطيع البحث عنها علي الإنترنت

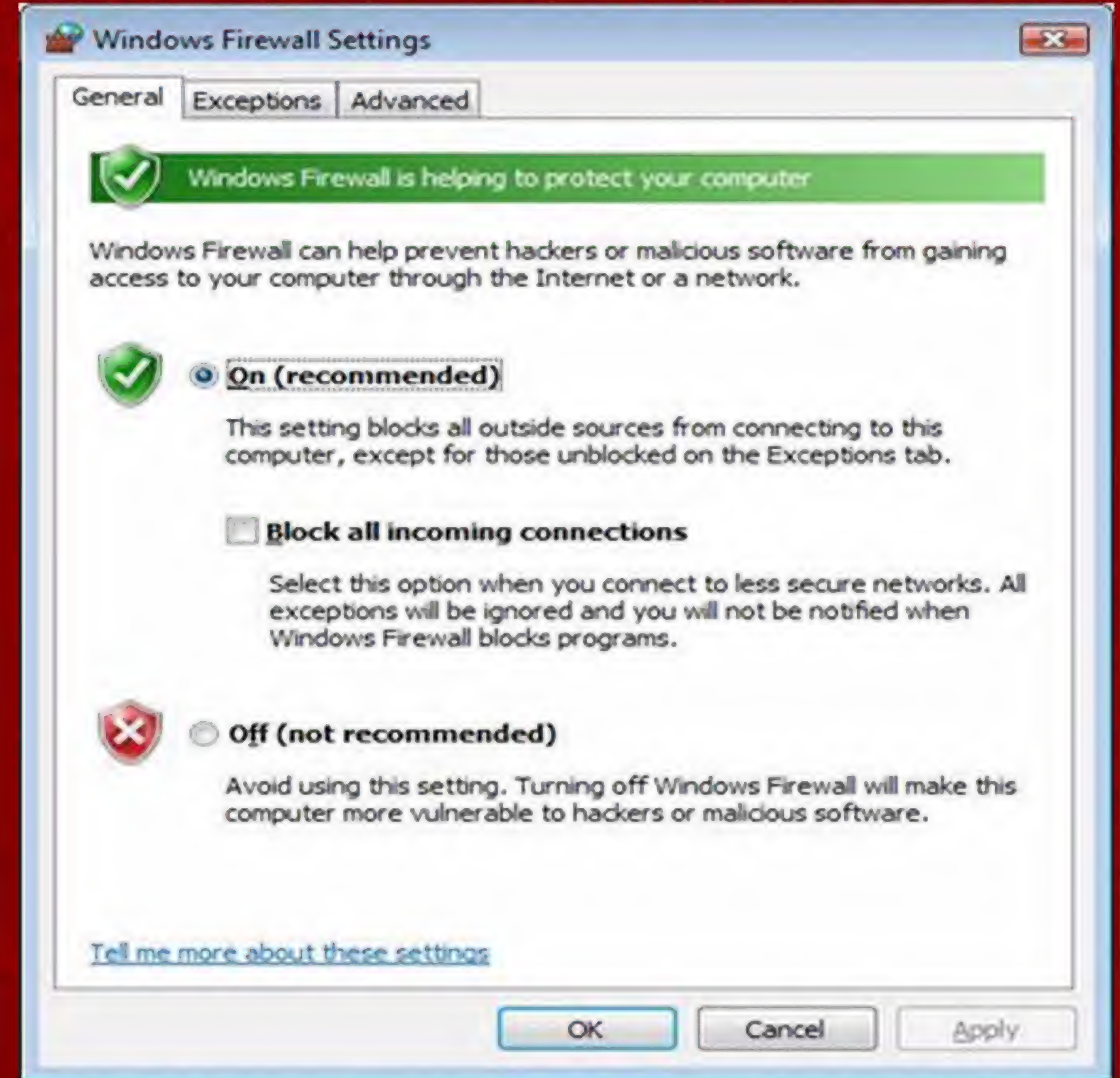
Layer 3

Troubleshooting

Layer 4: Transport

هل لديك جدران نارية Firewall علي جهازك أو تستخدمه في شبكتك

هذه الطبقة و التي تسمي بطبقة النقل Transport layer هي عصب أو قلب نموذج OSI لأنها حقيقة التي تربط بين الطبقات العليا و الدنيا من هذا النموذج و لذلك تختص مشاكلها غالبا في عدم أو صعوبة تدفق البيانات و عمليا لابد أن تتأكد جيدا من سلامة برمجيات أو أجهزة الفايروول لديك و أنها قد تم إعدادها بالشكل الذي تريده و مشكلة إنقطاع الإنترنت بسبب منع الفايروول لتدفق بيانات الإنترنت هي من أكثر مشاكل الإنترنت شيوعا و الفايروول لدينا أما أن تكون شبكية مثل Symantec أو forefront أو محلية مثل برمجيات الفايروول العادية المدمجة في نظم التشغيل أو برمجيات مستقلة مثل Kaspersky أو Norton client



و إما أن تكون برمجية مثل ISA و Symantec أو أجهزة مثل PIX و Bluecoat أوراوترات تم إعدادها لتلعب دور الفايروول

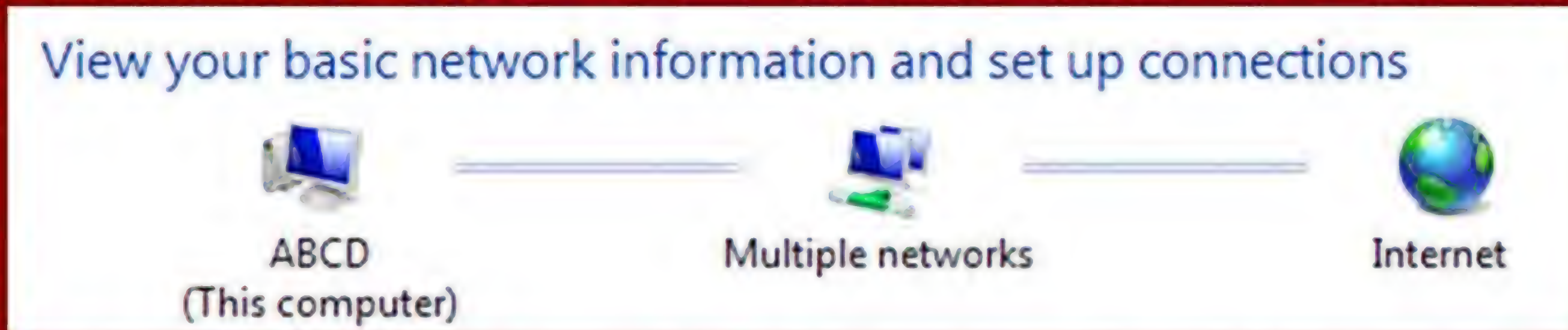
Layer 5 through 7

Troubleshooting

Layer 5-7: Upper Layers

هل تستطيع الإتصال بالإنترنت بواسطة المتصفح أو أي برمجيات أخرى

في هذه الطبقات و التي أطلقنا عليها اسم الطبقات العليا سنحاول أن نتأكد من عمل البرمجيات التي علي الجهاز فقد يكون كل شيء علي ما يرام من الكابل الي كارت الشبكة و السويتش و مرورا بالراوتر و الفايروول و هنا يجب أن تبحث عن المشكلة الموجودة في برمجيات الإتصال و غالبا تكون بسبب فيروس و انتهاء رخصة برنامج الإتصال أو التصفح أو احتياجه لتحديثات ضرورية أو ربما لأنك أخطأت في كتابة اسم الموقع أو ما يسمى بمشكلة HTTP قد يكون أيضا نظام التشغيل غير مستقر و يحتاج تحديثات ضرورية أو رقعات أمنية بعد انتهائك من تتبع هذه الأخطاء فلا بد أن تكون نجحت في القدرة علي إعادة الإتصال بالإنترنت



في النهاية اعلم جيدا أنك و أنا معك قد نجد لبس عند محاولتنا للزج بإحدى المشاكل في الجهة أو الطبقة المسؤولة عنها لكن عندما تحدد المشكلة و تحدد الحل فصدقني سيزول هذا اللبس .

و قبل أن أتركك فإننا أعترف أنني لم أقدم لك شيئا جديدا لكن بالتأكيد قدمته لك بطريقة جديدة نوعا ما و أعتقد أنه بواسطة فهم هذا النموذج الفهم الصحيح فإنك تستطيع بإذن الله أن تربط و تجمع شتات كثير من معلومات الشبكات التي تم نشرها في عشرات الشهادات و مئات الكتب و الاف المقالات و ذلك في خطوط عريضة تستطيع أن تجعل من كل واحدة منها كتاب

و لا أدعي أيضا أنك ستكون خبيرا في فهم كل مجالات الشبكات لكن ما أقصده أنك ستستطيع بعد فهم نموذج OSI فهما صحيحا أن تربط ما فهمته حتي الآن في الشبكات بما تريد أن تفهمه و أن تعرف ما موقع ما فهمته في خارطة طريقك للشبكات

أتمنى يوما أن أجد كتاب عربي كامل عن هذا النموذج يشرح كل ما فيه بشكل تتعانق فيه السطور النظرية مع التطبيقات العملية ليكون كل ما نعرفه في الشبكات مرتبا طبقا للطبقات و ليس طبقا للشهادات المعروفة ليكون مرجعا لأي من يريد أن يلج عالم الشبكات من أوسع أبوابه

أساسيات التعامل مع الـ intrusion detection and prevention systems

شريف مجدي

مثال 1 : هناك هجوم يستهدف الـ http server و بعد تحليل هذا الهجوم من قبل الخبراء وجدوا الاتى .
حتى يستطيع المهاجم اتمام هذا الهجوم يجب ان يرسل packet لها هذه الصفات تحوى على هذه الـ string 100.1.1.10." .

هنا يتم تصميم signature لهذا الهجوم و فى هذه الحالة نصمم هذه الـ sig بحيث تقوم بالبحث داخل الـ packet عن الـ string السابق و يقوم الـ IPS بتمرير جميع الترافيك على هذه الـ sig لتقوم بفحصه و تتأكد من انه خالى من هذا الكود الخبيث الذى فى هذه الحالة هو 100.1.1.10 , هذا مثال بسيط لتوضيح الامر فقط فهناك هجمات شديدة التعقيد و الـ sig التى تقوم بالتصدي لها اكثر تعقيدا

الان نفترض ان هناك هجوم و يقوم الـ IPS بعرض هذا الهجوم على كل الـ sig. و جاء دور الـ sig. المخصصة لكشف هذا الهجوم ماذا سيحدث ؟
سيحدث ما يسمى بالـ sig triggering اى تم التحقق من ان هناك هجوم جارى و هنا تقوم الـ sig بعمل عدة اشياء

1 سريعا سيقوم بارسال alert و تخزينه فى الـ event store حيث يستطيع مراقب الشبكة ان يعرف ان هناك هجوم جارى

2 تقوم باتخاذ قرار حسب طريقة اعداد الـ sig فمثلا عندما يتم تصميم الـ sig يجب ان تحدد ماذا يفعل هذا الجهاز اذا حدث الهجوم



فى هذا المقال سأتكلم عن موضوع مهم فى عالم الـ security و هو اساسيات التعامل مع اجهزة منع و كشف المتطفلين فى الشبكة (sensors) و الذى يساعد على بقاء الشبكة امنه من الهجمات الخارجيه

قبل ان ابدأ احب ان اوضح بعض المصطلحات سريعا :
IPS : هو عبارة عن جهاز يقوم بتحديد الهجمات و التصدي لها وامكانيه تعديلها و تسجيلها لهذا فيجب ان يكون فى مسار البيانات

IDS : بعكس الاول تماما فهو قادر فقط على تحديد الهجمات و ارسال تحذير الى workstation

in-line mode : هى الوضعية المثلى لجهاز الـ IPS و فى هذه الوضعية يكون الجهاز فى مسار تدفق البيانات اي ان البيانات يجب ان تمر من خلاله.

promiscuous mode هو الوضع الخاص باجهزه الـ IDS ويتم توصيل الجهاز الى span port or Remote الى الـ switch ليستطيع الجهاز ان يقوم بعمل فحص للبيانات التى تمر اليه و ليس من خلاله مثل حاله السابقه , و ايضا من الممكن ان يستعمل الـ IPS هذا الوضع

اليه عمل هذا الجهاز و طرق تعرفه على الهجمات :
يعتمد هذا الجهاز على اكثر من طريقة و سنتعرف على اهمها فى هذا المقال

- 1- signature-based
- 2- policy-based
- 3 anomaly detection

الطريقة الاولى تعتبر الطريقة الاساسية التى يتم الاعتماد عليها و هى تقوم بتحديد الهجمات الشائعه (common attack) , وتعتمد على عمل signature لكل هجمه

• هل يقوم بارسال alert فقط ؟

• هل يقوم بمنع ال packet التى تحتوى على هذا الهجوم فقط ؟ (طبعا لا اريد ان اهيئ ذكاء القارئ و اقول ان هذا فى حالة ال line mode ^{بسرته و سريته} in اى يجب ان يكون الجهاز IPS)

• هل يقوم بمنع المهاجم منعاً كاملاً ؟

• هل يقوم بارسال RST لقطع الاتصال

• هل يقوم بعمل log للهجوم (اقصد هنا عمل capture له و من ثم عرضه عن طريق wireshark مثلا)

و خيارات اخرى كثيرة وذلك حسب الحاجة فهناك هجمات ليست خطيره يكفى ارسال alert و هجمات اخرى خطيرة فيجب فى هذه الحالة اتخاذ اكثر من قرار , منع الهجوم و المهاجم

انواع ال sig :

1 - builtin sig.

2 - tuned sig.

3 - customized sig.

النوع الاول هو الشكل الاساسى لكل sig من دون تغيير اى اعدادات او تغيير شئ بها , و ياتى الجهاز بحوالى sig 2000 لتحديد معظم الهجمات الشائعه و جميعها تم تصميمه من قبل سيسكو

مثال 2 : عندنا شبكة تحتوى على عدة سيرفرات ftp و فى نفس الوقت هناك هجوم منتشر يستهدف ال ftp server و هذا الهجوم مازال فى 0 day و لم يتم اصدار اى sig له من سيسكو

الان ماذا نفعل هل نترك الشبكة مهدده حتى يتم اصدار ال sig ؟ طبعا لا , سنقوم بعملها بنفسنا , اولاً نبحث و نقرأ كثيراً بخصوص هذا الهجوم و بعد البحث و جدنا ان هذا الهجوم يميزه هذه الكلمة "FtP AtTAck"

الان نقوم بتصميم sig بسيطة جدا تقوم بالبحث عن هذه الكلمة و منع ال packet و اجراء اى action من الذين تم ذكرهم سابقاً لمنع هذا الهجوم مؤقتاً لحين نزول sig من قب سيسكو

signature engines :

بعد ان علمنا ان ان هناك عدد كبير من ال sig لابد من تنظيم هذا العدد بطريقة معينة حتى لا يحدث اى تاخير ينتج من فحص الترافيك و هنا تم تقسيم ال sig الى مجموعات متعددة , كل مجموعه تسمى engine و تحتوى هجمات تستهدف هدف معين فمثلاً تم تجميع الهجمات التى تهدد ال http ووضعهم فى engine واحد , و يتم تشغيل الجهاز يتم تحميل كل engine فى ال ram كى يستطيع الجهاز تمرير الترافيك اليها

ويكون ذلك in-parallel و ليس ان in-serial اى سيتم عرض ال packet على جميع ال sig فى ال engine الواحد فى وقت واحد .

وهذه بعض ال engine

ATOMIC Signature Engines : تهتم هذه المجموعه من ال sig بالهجمات التى تتم عن طريق packet منفردة

FLOOD Signature Engines : هجوم ال DOS & DDOS

SERVICE Signature Engines : بعض الخدمات المختلفة و البرتوكولات العامة

STRING Signature Engines : تقوم بعمل match ل string معينه عن طريق regular expression مايسمى بال fingerprint

TROJAN Signature Engines : تكشف التروجان

TRAFFIC Signature Engines : بعض البروتوكولات

AIC Signature Engines : مخصصه لل deep inspection for HTTP and FTP only

STATE Signature Engine : نوع مخصص لل state protocols

META Signature Engine : اما هذا فيقوم بكشف الهجوم الذى يسبقه عدة هجمات اخرى مثل NIMDA attack

NORMALIZER Engine : خاص بال anomaly detection

: Policy-Based

تعتمد هذه الطريقة على أولويات الشبكة و الترافيك المسموح له بالمرور فى الشبكة فمثلا اذا كان هناك مجموعه سيرفرات http فيمكن ان تتبع سياسته تمنع مرور اى نوع اخر من الترافيك مثل ال ftp مثلا, ففى هذه الحالة نقوم بعمل policy تمنع اى ترافيك من المرور سواء كانت خطيرة ام لا و ارسال alert الى ال event store و السماح فقط لل HTTP

: Anomaly-detection

هذه الطريقة جديده على cisco sensors و تم تصميمها لتعمل جنبا الى جنب مع ال signature-based method

وهدف الرئيسى منها هو منع انتشار ال worms فى الشبكة , فيتم اتباع طريقة معينة لمعرفة ال normal traffic و ارسال alert فى حاله اى تغيير عن normal الذى تم التعارف عليه

(POSFP (passive operating system fingerprint هى تقنيه جديده فى ال IPS V.6 تقوم بالتعرف على نظام التشغيل للضحية

مثال 5 : قام ال IPS بالتعرف على هجوم على linux server يملك هذا ال ip 10.10.10.10 عندها يقوم ال IPS بالبحث فى قاعده بيانات يمتلكها ليتعرف على نوع نظام التشغيل الخاص بالضحية .

فى هذه الحاله سيجده مثلا linux RedHat ووجد ايضا ان هذا الهجوم يستهدف ال ISA server و لن يسبب اى ضرر للينكس عندها يعرف انه ليس من الضرورى ان يقوم باراسال alert وذلك تقريبا من عدد الانذارات لسهولة التحقيق فيهم فيما بعد , او من الممكن ان يرسل alert ولكن سيكتب بها "not relevant"

اخيرا احب ان اتكلم عن best IPS location

يعتمد هذا الموضوع حسب ظروف الشبكة التى تريد حمايتها و لكن الشائع هو خلف الراوتر او الفايروال ولكن هذا لا يمنع انه فى بعض الحالات يمكن وضعه امام ال firewall

الموضوع مازال اكبر من ذلك و ان شاء الله نتكلم عن خواص اخرى فى هذا الجهاز الرائع

نعود الى ال alerts مرة اخرى و كما قلنا يقو م ال IPS بوضع هذه ال alert فى ال event store عند حدوث هجوم

واريد هنا ان قوم بشرح مصطلح بسيط هو alert severity و اذا ترجمنا هذه الكلمة نجد المعنى هو شدة الانذار بمعنى اخر ما هو مستوى الهجوم الذى سبب هذا الانذار , و هذه هى المستويات

low – medium – high – informational

ويمكنك ان تقوم بتغيير ال default لكل sig حيث تقوم بعمل alert بالمستوى الذى تراه انت مناسب و من الممكن تركه كما هو على حسب وجه نظر سيسكو , فى بعض الاحيان يجب تغييره

: positive and negative alerts

ناتى هنا الى مصطلحان جديدان و هو ال false positive and negative alarms فإذا كان المخترق بارع من الممكن ان يقوم بخداع ال sig و يتجنب الكشف و يستطيع تمرير الترافيك الخبيث الى داخل الشبكة و هنا نطلق هذا المصطلح false negative

مثال 3 : اريد ان اقوم ببدء هجوم على شبكة محمية عن طريق IPS device و بعد البحث وجدت ان هناك sig ستقوم بكشف هذا الهجوم لنقل مثلا لان الهجوم يميزه هذه الكلمة "ATTack" عندها اقوم انا بعمل مراوغه بسيط و اخدع الجهاز و تغير هذه الكلمة الى تميز الهجوم الى "attACK" عندها سيتم الهجوم , و لكن خداع ال IPS يحتاج الى مخترق بارع .

اما ال false positive فهو عندما يرى ال IPS ترافيك سليمة و غير خطيرة و يعتقد انها هجوم و يقوم بمنعها . والسبب فى ال false positive & false negative هو التصميم السيء لل signature هذا بالنسبة لل signature-based , أما النوعان

الاخران



خلق عليه عهد

أنس الأحمـد

بسم الله الرحمن الرحيم

وحين نعود إلى أساسيات ديننا الحنيف لوجدنا أن الأخلاق مقدمة حتى على العبادات الأساسية ففي حديث رسول الله صلى الله عليه وسلم بما معناه عن المفلس الذي يأتي يوم القيامة بصوم وصلاة ويأتي وقد شتم هذا وقذف هذا وأكل مال هذا فتؤخذ من حسناته وتعطى لهم ثم تؤخذ من سيئاتهم وتطرح عليه ثم يطرح بالنار وكذلك قوله تعالى حين يبين صفات عباد الرحمن التقاة بعد بسم الله الرحمن الرحيم (وعباد الرحمن الذين يسيرون على الأرض هونا وإذا خاطبهم الجاهلون قالوا سلاما والذين يبيتون لربهم سجداً وقياماً)

ونلاحظ أن التعفف عن الجاهلين وهو خلق سبق الصلاة وقيام الليل وهو عبادة كذلك يجب ألا نكتفي بمجرد الفخر بما أننا أصحاب حضارة وإنجازات يعترف بها العالم إلى اليوم فحضارة أجدادنا استمرت بأخلاقهم وحتى إنجازاتهم العلمية ازدهرت في وقت رفع فيه لواء الأخلاق .

طبعاً هذه دعوة لدمج الأخلاق في كل نواحي حياتنا بما فيه العلم والعمل لأن ذلك يعني الأمانة في منح ما نملكه من معلومة أو مجهود وهذا يعود بالنفع على الجميع

أرجو من الله أن يلهمنا جميعاً صلاحاً وتقوى في الدنيا والآخرة ويمدنا بالقوة لفعل الخير ونشره

اعذروني إخوتي جميعاً إذا كانت مقالاتي مملة بعض الشيء ولا تدخل كثيراً في صلب اختصاص المجلة ولكنني أظن أن جانباً كهذا الجانب لوبقي في مجلتنا فمن الممكن أن يساهم نوعاً ما بتأكيد رسالة المجلة التي تريد أن توصلها ألا وهي الخير ثم الخير ثم الخير للجميع . وانطلاقاً من هذه النقطة وتكملة لمقالة العدد السابق التي أكدت على ضرورة اقتران العلم بالعمل أود أن أؤكد على عامل يتكامل مع العاملين السابقين ولا نستطيع عزله عنهما .

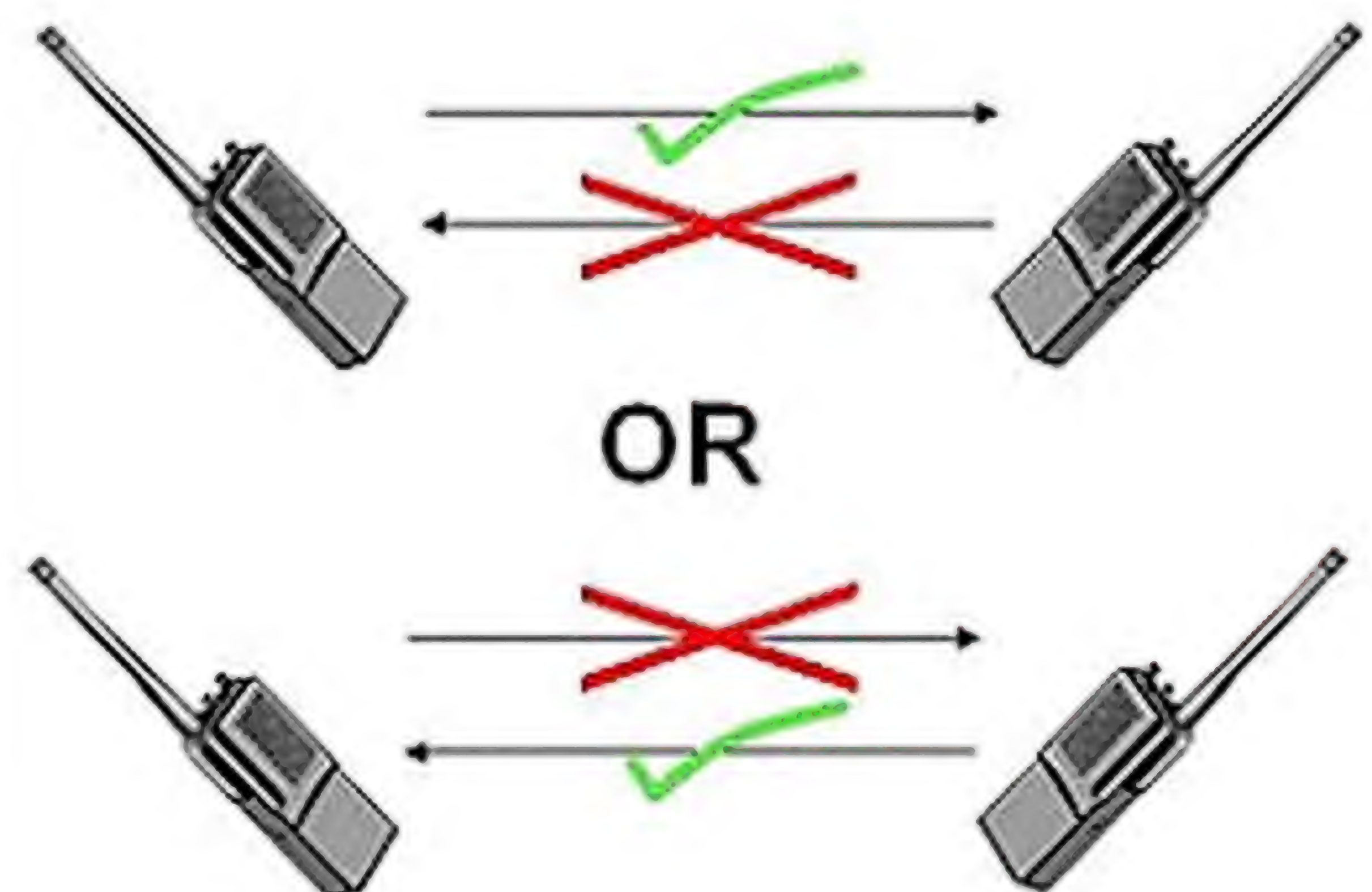
حين نتحدث عن مفهوم الأخلاق قد يخيّل للبعض أنها إحدى قصص شهرزاد القديمة التي انقرضت أو المدينة الفاضلة التي لم تتجاوز أسوارها حدود ورق الفلاسفة وكتاباتهم وأن عصرنا المادي الحالي يعترف بمقدار الإنجازات والمكاسب التي يحققها الإنسان بغض النظر عن الطريقة أو الأسلوب وبتجاهل مقدار الضرر الذي سببه لمن حوله .

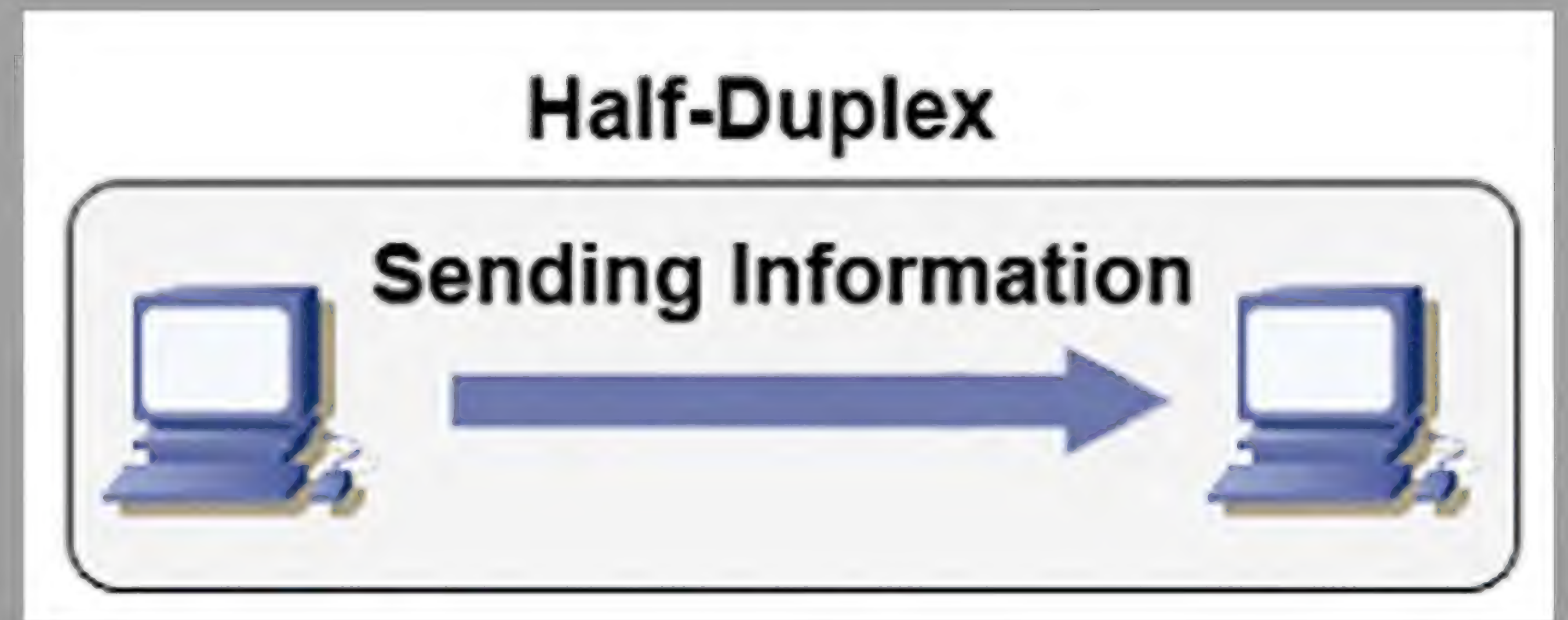
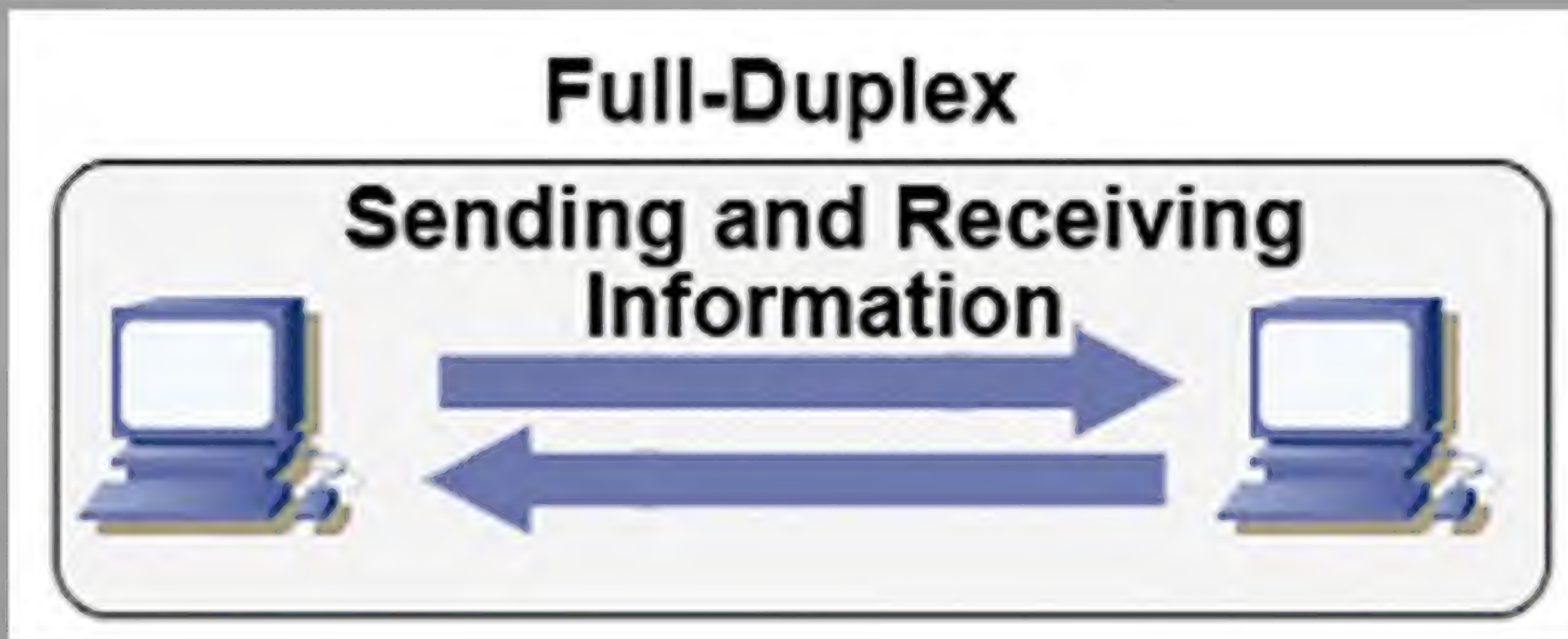
أخوتي في الله قد يتراءى لنا من خلال مراقبتنا لمن حولنا أن كلام هؤلاء يعتريه شيء من الصحة ولكن صدقوني أن ذلك مجرد أوهام فالإنجازات لاتقاس بالماديات فقط ولا أقصد بكلامي هذا ترك الإنجازات العملية ولكن فقط القيام بعملية اقتران بسيطة بين الأخلاق وكل ما ننجزه في حياتنا فذلك يسهم في زيادة محبة الله والناس لنا ولإنجازاتنا وبالتالي إضفاء المزيد من النجاح والاستمرارية .

الإرسال والاستقبال من خلال الكابل

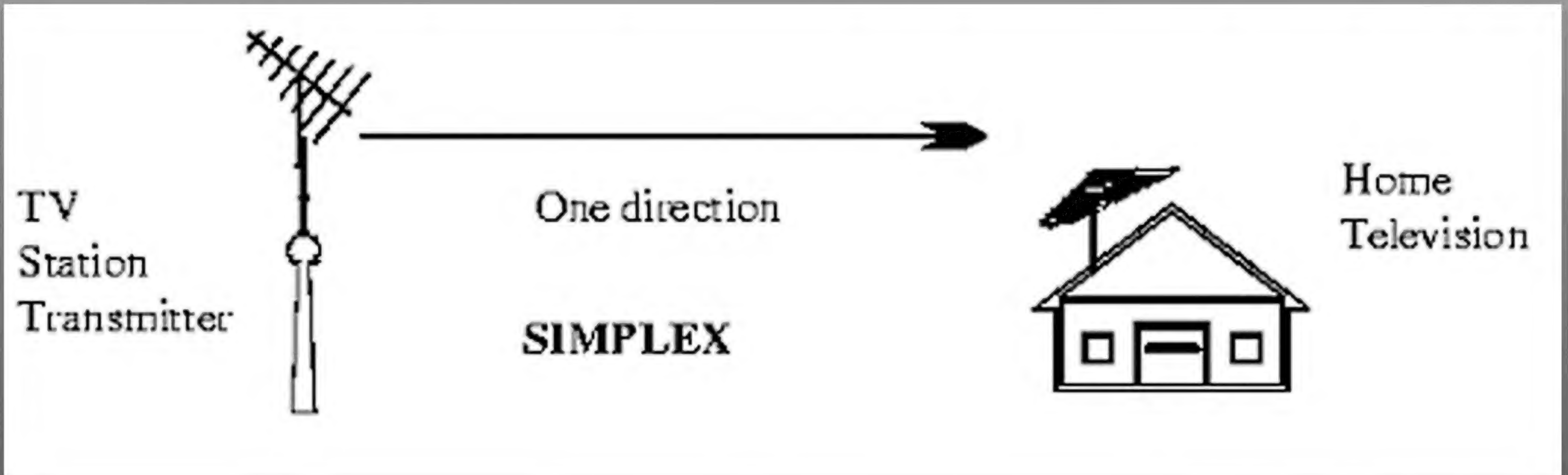
عندما كنت أستقل القطار من محطة بنها الي محطة منوف حيث توجد كليتي كان القطار ينتظر احيانا في محطة الباجور كي ينتظر القطار المقابل لأن شريط القطار فردي لا يتحمل قطارين في نفس الوقت ودعنا نسمي تلك الطريقة half duplex وعلي العكس فإن المسافة ما بين محطة بنها الي الزقازيق كان شريط القطار مزدوج يسمح لقطارين متقابلين بالمرور وسنسمي تلك الطريقة full duplex هذه هي فكرة ارسال و استقبال الإشارات من خلال الكابلات و مدي تطورها علي مدي الزمن حيث ان half duplex هي نقل الإشارة اياها فقط او ذهابا فقط ولا يمكن الإرسال و لإستقبال في نفس الوقت مثل أجهزة الشرطة اللاسلكية حتي انك تسمع كلمة ” حول “ بعد انتهاء كل فقرة ليخبر الطرف الآخر انه انهى حديثه والمسار فارغ.

full duplex وهي تسمح بنقل الإشارة ذهابا و ايابا في نفس الوقت اي ترسل وتستقبل مثل جميع أنظمة الإتصال التي تستطيع ان تتحدث وتسمع في نفس الوقت والتي تشمل أيضا منظومات شبكات الحاسوب .





واضافة لذلك فإنه يوجد نظام يدعي simplex يسمح فقط بالإرسال من جهة لأخري ولا يسمح اطلاقا بالعكس مثل الإرسال التلفزيوني واتصال الطابعات بالحاسوب



ولارسال اشارة داخل الكابل بمدي ترددي اعلي من نطاق الكابل في الشبكات المحلية فإنه يتم استخدام زوجين من كل اربع ازواج للإرسال والإستقبال زوج يرسل والأخر يستقبل ومن الممكن ان تعتبر المسار مثل طريق السيارات تسير فيه سيارة واحدة فقط كل فترة زمنية خلال مسافة من الممكن ان نستغل تلك الترة الزمنية ونجعل ثلاث سيارات مثلا تسير في نفس المسافة في نفس الزمن اي ثلاث سيارات كل ثانية بدلا من واحدة كل ثانية ولكن قطعاً سيأتي يوما وتزداد السيارات عنا لابد من عمل طرق اخري اي ننشيء مسارين اضافيين احدهما اياها والأخر ذهابا ولكن الا تلاحظ احيانا انه في اوقات الذروة تجد ان احد جانبي الطريق مشغول والأخر المقابل فارغ .. فلم لا نستغل هذا الفارغ وهذه هي فكرة جيجا ايثرنث وهو استخدام كافة المسارات ذهابا وايابا لإرسال واستقبال الإشارات وهي طريقة رائعة مكنتنا من ارسال ترددات تصل الي 1000 ميغا بت لكل ثانية علي كابل ذو مدي ترددي 100 هرتز اي من خلال كابل من الفئة الخامسة ومشتقاتها cat 5





لا شك أن لكل مشكلة حل ، ويمكن حل المشكلة بسهولة إذا تم معرفة السبب . حيث أن اكتشاف المشكلة وإصلاحها بدقة وبسرعة لا يكون بمحض الصدفة فحسب ، وإنما يتطلب اتباع إجراءات محددة . وفي مجال الشبكات ، هناك خطوات فنية يجب اتباعها بالترتيب ، ولا بد أن تعرف تفاصيل كل خطوة وما عليك أن تفعله فيها لتتمكن من الانتقال للخطوة التي تليها ، حتى تصل للخطوة الأخيرة وبها تكون المهمة اكتملت وأنت متأكد من سلامة وفعالية العمل الذي قمت به

هناك ثلاثة مصادر رئيسية تستطيع أن تجمع منها المعلومات ، وهي :

+++ جهاز الكمبيوتر +++

وذلك عن طريق رسائل الخطأ التي يظهرها النظام عندما تحصل المشكلة ، ويمكن تفسير هذه الرسائل من خلال مراجعة الويب سايت (Website) للشركة المصنعة لنظام التشغيل المثبت على جهاز الكمبيوتر .

+++ الشخص الذي لديه المشكلة +++

تُعتبر مهارات التواصل الفعال مع المستخدم ذات أهمية كبيرة عند جمع المعلومات ، وفي غالب الأحيان يكون المستخدم ذو معرفة محدودة بالكمبيوتر وهذا يجعل الأمر أكثر صعوبة لمعرفة ماهية المشكلة ، ولكن من خلال مقابلة المستخدم وطرح عليه بعض الأسئلة فإنه سوف يخبرك ماذا حدث ، وما كان يحاول أن يفعله ، وما هي الأمور التي لا تعمل .

وأهم المعلومات التي يجب أن تسأل عنها في هذه المقابلة هي :

/// مرات تكرُّر الخطأ :

هل يحدث الخطأ على فترات منتظمة أم بشكل متقطع هل يحصل يومياً أم أسبوعياً أم شهرياً ؟
/// التطبيقات المستخدمة :

من المهم أن تعرف ما هي البرامج التي كانت تعمل وقت حدوث المشكلة .

في هذا المقال ، سوف نتحدث عن الخطوات التسع والتي تعتمد عليها منظمة CompTIA في منهاج شهادة Network + كمنهجية لحل مشاكل الشبكة .

- * جمع المعلومات عن طريق التعرف على الأعراض والمشاكل الموجودة .

- * تحديد الأماكن التي بها عطل في الشبكة .
- * معرفة آخر التغييرات في الشبكة .
- * تكوين فكرة عن أكثر سبب محتمل .
- * قد تحتاج إلى رفع المشكلة إلى سلطة تنفيذية أعلى إذا كانت المشكلة خارج مسؤوليتك .
- * وضع خطة عمل للبدء بالحل ، مع الأخذ بالاعتبار تحديد التأثيرات الكامنة وراء كل خطوة .
- * تنفيذ الحل ، ثم اختبار فاعليته بتفحص الأجزاء التي كانت متضررة .
- * معرفة نتائج التفحص وتأثيرات الحل .
- * وأخيراً ، سجل الحل بكتابة تقرير عن كامل العملية .

الخطوة (1): جمع المعلومات عن طريق التعرف على الأعراض والمشاكل الموجودة

تكون الخطوة الأولى في عملية إصلاح المشكلة هي معرفة المشكلة الموجودة من خلال العلامات التي تدل عليها . ولكي تحصل على المعلومات فإنه يجب أن يكون لديك معرفة بنظام التشغيل المستخدم ، ومهارات التواصل الشخصية ، وشيئاً من الصبر .

منهجية حل مشاكل الشبكة

/// المشكلات الماضية :

هل حدثت هذه المشكلة من سابق ؟ هل كان لها علاقة بإحدى المشكلات قد حصلت في الماضي ؟

/// تغييرات من المُستفهِم :

إضافة أو إزالة برنامج أو أحد مكونات الكمبيوتر قد يكون له تأثير سلبي على أمور أخرى كانت تعمل بشكل سليم من قبل . استفسر من المستخدم فيما إذا فعل أي تغييرات في الجهاز .

/// رسائل الفطا :

تعرض أنظمة التشغيل رسائل خطأ لإبلاغ المستخدم بالمشكلة الحاصلة في هذا الوقت . اسأل المستخدم لكي يخبرك ما هي الرسالة التي تظهر له .

+++ خبم تان وملاحظاتان الشخصية +++

تلعب أساليب الملاحظة الفنية باستخدام حاسة النظر والسمع والشم دوراً كبيراً في عملية اكتشاف الخطأ ، وبذلك فإنك تستطيع أن تجد المشكلة وهي صغيرة قبل أن تصبح مشكلة كبيرة .

وكمثال على هذه النقطة ، مشكلة انفصال الكيبل المتصل بكرت الشبكة فإنك سوف تلاحظ انطفاء أزرار الضوء (LED) الموجودة على جانبي منفذ الكرت ، وعند قيامك بإعادة تثبيته جيداً فستري أن هذه الأزرار تومض دليل على أن التوصيل صحيح والاتصال يعمل بشكل سليم .

*** أسئلة عملية ذات أهمية ***

بغض النظر عن الطريقة التي تستخدمها لجمع المعلومات عن المشكلة الحاصلة ، يجب أن تبحث عن إجابات لبعض الأسئلة الهامة .

عندما تبحث في مشكلة تأكد من معرفة إجابات الأسئلة التالية لكي تصل لجذر المشكلة :

□ هل المشكلة تخص جهاز كمبيوتر واحد أم أن كامل الشبكة معطلة ؟

□ هل هناك مشكلة في تصفح موقع معين ؟ أو نوع معين (أي http ، https ، ftp) ؟

□ هل يمكنك عمل ping للتأكد من سلامة اتصالك بالجهاز الآخر ؟

□ هل تأكدت من إعدادات الاتصال من خلال الأمر ipconfig /all ؟

□ هل المشكلة تحدث باستمرار أم أنها متقطعة ؟ وهل لها أوقات معينة ؟

□ هل حدثت نفس المشكلة من قبل ؟

□ هل تم إزالة أو تركيب أي من معدات الشبكة حديثاً ؟

□ هل تم تثبيت أي تطبيقات جديدة على الشبكة ؟

□ هل حاول أحد ما إصلاح المشكلة ؟ إذا كان كذلك ، فماذا فعل ؟

□ هل يوجد أي مستندات أو تقارير سابقة تتعلق بالمشكلة أو بالتطبيقات أو الأجهزة المرتبطة بالمشكلة ؟

عندما تجد الإجابة على هذه التساؤلات فإنك بذلك تكون كوّنت فكرة أفضل عن حقيقة المشكلة الموجودة بالضبط . وبهذا فإن المرحلة الأولى قد انتهت ويأتي بعدها دور المرحلة الثانية .

في العدد القادم سوف نكمل حديثنا بإذن الله عن الخطوات الأخرى دمتم بخير

منهجية حل مشاكل الشبكة

علاء مازن عدوي



يعتبر الجبر البوليني هو الأب الشرعي للتكنولوجيا الرقمية التي انبثقت منها الكمبيوتر و تكنولوجيا الاتصالات الحديثة , و تتمحور فكرة الجبر البوليني هو تحويل أي رقم الي رقمين فقط هما 0 و 1 و بتبسيط أكثر و بعيدا عن الجبر البوليني , هو تحويل أي شيء في هذه الدنيا الي احتمالين فقط هما نعم أو لا – ابيض او اسود ,, أو اي احتمالين متضادين لا ثالث لهما ك مغلق مفتوح – فوق تحت – يمين يسار و يتم تقريب اي احتمال آخر الي هذين الاحتمالين

تصور مثلا بعد أن كنت تتعامل مع الف لغة تترجم بينهم ثم تفاجأ أنك ستتعامل فقط مع لغتين ,, أظن أنك سيغمي عليك من الفرحه

حيث تتمثل الألف لغة في الحروف و الأرقام بكل لغات العالم مع أشكال الصور و الفيديو و كل شيء ,, هذا كله سيتم تحويله بطريقة ما الي رقمين فقط أو احتمالين فقط هما 0 , 1

هل الأمر بهذه البساطة ؟ لا اطلاقا لكن تكفيك هذه الأساسيات لتفهم سر النمو الغير طبيعي لتكنولوجيا الاتصالات و المعلومات و الإلكترونيات

فقد كانت هذه الفرضيات أو النظريات أساس ما تراه حاليا من تكنولوجيا و تم استغلالها فيزيائيا و تحويلها الي اجهزة و الالات لا مجال لسرد طريقة عملها في صفحات

نسخة أقل من بسيطة عن ASCII

و غالبا و بما انك تقرأ هذا الموضوع و وصلت غير مجبرا الي هذا السطر فأنت علي علم بأساسيات التحويل بين الأرقام العادية و أرقام الثنائية او التحويل بين النظام التماثلي الي النظام الرقمي و لكن ربما يغيب عنك تحويل الحروف الي هذا النظام

و التحويل من الحروف الي النظام الرقمي كي تستطيع الأجهزة الرقمية التعامل معه يتم باستخدام طريقة تحويل تسمى the American Standard Code for Information Interchange ^{مصراته ليبيا} ASCII CODE النظام الأمريكي للتحويل وفق الجدول التالي :

ASCII TABLE

Decimal	Hexadecimal	Binary	Octal	Char	Decimal	Hexadecimal	Binary	Octal	Char	Decimal	Hexadecimal	Binary	Octal	Char
0	0	0	0	[NULL]	48	30	110000	60	0	96	60	1100000	140	`
1	1	1	1	[START OF HEADING]	49	31	110001	61	1	97	61	1100001	141	a
2	2	10	2	[START OF TEXT]	50	32	110010	62	2	98	62	1100010	142	b
3	3	11	3	[END OF TEXT]	51	33	110011	63	3	99	63	1100011	143	c
4	4	100	4	[END OF TRANSMISSION]	52	34	110100	64	4	100	64	1100100	144	d
5	5	101	5	[ENQUIRY]	53	35	110101	65	5	101	65	1100101	145	e
6	6	110	6	[ACKNOWLEDGE]	54	36	110110	66	6	102	66	1100110	146	f
7	7	111	7	[BELL]	55	37	110111	67	7	103	67	1100111	147	g
8	8	1000	10	[BACKSPACE]	56	38	111000	70	8	104	68	1101000	150	h
9	9	1001	11	[HORIZONTAL TAB]	57	39	111001	71	9	105	69	1101001	151	i
10	A	1010	12	[LINE FEED]	58	3A	111010	72	:	106	6A	1101010	152	j
11	B	1011	13	[VERTICAL TAB]	59	3B	111011	73	;	107	6B	1101011	153	k
12	C	1100	14	[FORM FEED]	60	3C	111100	74	<	108	6C	1101100	154	l
13	D	1101	15	[CARRIAGE RETURN]	61	3D	111101	75	=	109	6D	1101101	155	m
14	E	1110	16	[SHIFT OUT]	62	3E	111110	76	>	110	6E	1101110	156	n
15	F	1111	17	[SHIFT IN]	63	3F	111111	77	?	111	6F	1101111	157	o
16	10	10000	20	[DATA LINK ESCAPE]	64	40	1000000	100	@	112	70	1110000	160	p
17	11	10001	21	[DEVICE CONTROL 1]	65	41	1000001	101	A	113	71	1110001	161	q
18	12	10010	22	[DEVICE CONTROL 2]	66	42	1000010	102	B	114	72	1110010	162	r
19	13	10011	23	[DEVICE CONTROL 3]	67	43	1000011	103	C	115	73	1110011	163	s
20	14	10100	24	[DEVICE CONTROL 4]	68	44	1000100	104	D	116	74	1110100	164	t
21	15	10101	25	[NEGATIVE ACKNOWLEDGE]	69	45	1000101	105	E	117	75	1110101	165	u
22	16	10110	26	[SYNCHRONOUS IDLE]	70	46	1000110	106	F	118	76	1110110	166	v
23	17	10111	27	[ENG OF TRANS. BLOCK]	71	47	1000111	107	G	119	77	1110111	167	w
24	18	11000	30	[CANCEL]	72	48	1001000	110	H	120	78	1111000	170	x
25	19	11001	31	[END OF MEDIUM]	73	49	1001001	111	I	121	79	1111001	171	y
26	1A	11010	32	[SUBSTITUTE]	74	4A	1001010	112	J	122	7A	1111010	172	z
27	1B	11011	33	[ESCAPE]	75	4B	1001011	113	K	123	7B	1111011	173	{
28	1C	11100	34	[FILE SEPARATOR]	76	4C	1001100	114	L	124	7C	1111100	174	
29	1D	11101	35	[GROUP SEPARATOR]	77	4D	1001101	115	M	125	7D	1111101	175	}
30	1E	11110	36	[RECORD SEPARATOR]	78	4E	1001110	116	N	126	7E	1111110	176	~
31	1F	11111	37	[UNIT SEPARATOR]	79	4F	1001111	117	O	127	7F	1111111	177	[DEL]
32	20	100000	40	[SPACE]	80	50	1010000	120	P					
33	21	100001	41	!	81	51	1010001	121	Q					
34	22	100010	42	"	82	52	1010010	122	R					
35	23	100011	43	#	83	53	1010011	123	S					
36	24	100100	44	\$	84	54	1010100	124	T					
37	25	100101	45	%	85	55	1010101	125	U					
38	26	100110	46	&	86	56	1010110	126	V					
39	27	100111	47	'	87	57	1010111	127	W					
40	28	101000	50	(88	58	1011000	130	X					
41	29	101001	51)	89	59	1011001	131	Y					
42	2A	101010	52	*	90	5A	1011010	132	Z					
43	2B	101011	53	+	91	5B	1011011	133	[
44	2C	101100	54	,	92	5C	1011100	134	\					
45	2D	101101	55	-	93	5D	1011101	135]					
46	2E	101110	56	.	94	5E	1011110	136	^					
47	2F	101111	57	/	95	5F	1011111	137	_					

للعلم فالأسكي قادر أيضا علي صياغة الصور و الفيديو و الصوتيات و أي صيغة تجدها علي الكمبيوتر